Evaluating the Effectiveness of Cybersecurity Protocols in SAP System Upgrades

ZAHOOR ALI SYED[1], EMMANUEL DAPAAH[2], GLORIA MAPFAZA[3], TICHAONA REMIAS[4], MUNASHE NAPHTALI MUPA[5]

[1, 2, 3, 4, 5] *HULT International Business School, Cambridge, Boston, Massachusetts, United States of America*

Abstract- ***This paper investigates the effectiveness of cybersecurity protocols during SAP system upgrades, focusing on both administrative and technical perspectives. As SAP systems are integral to numerous industries and increasingly targeted by sophisticated cyber threats, robust cybersecurity measures are essential during system upgrades to protect data integrity, confidentiality, and availability. The study begins by outlining the evolution of SAP systems and their significance in managing business processes and data across various organizational functions. It then delves into the critical role of administrators in planning, risk assessment, and stakeholder communication, highlighting their responsibilities in ensuring secure upgrades. From a technical standpoint, the paper addresses challenges such as software updates, data protection, and system integration. Technical solutions like encryption, data masking, and advanced authentication mechanisms are explored to safeguard sensitive information. The importance of intrusion detection systems and continuous monitoring is emphasized for real-time threat detection and response. Case studies illustrate both successful and breached SAP system upgrades, underscoring the necessity of comprehensive cybersecurity strategies. Successful upgrades, like those of Kenya Pipeline Company and Petroleum Development Oman, demonstrate the effectiveness of stakeholder engagement and rigorous security measures. Conversely, case studies involving breaches, such as the SolarWinds hacking incident, highlight vulnerabilities and the need for robust security protocols. The comparative analysis of administrative and technical perspectives reveals their complementary roles in managing SAP upgrades. Administrators focus on strategic planning and compliance, while technical teams implement and maintain security measures. The paper concludes with recommendations for a holistic approach to cybersecurity, integrating administrative policies with technical solutions to protect against evolving threats. Future research should focus on advancements in AI, machine learning, and quantum-safe encryption to enhance SAP system security.***

I. INTRODUCTION

The effectiveness of cybersecurity protocols in SAP system upgrades is a critical area of study given the pervasive use of SAP systems in various industries and the increasing sophistication of cyber threats (Akhtar and Feng, 2021). SAP systems, initially developed by SAP SE, have evolved significantly since their inception in the early 1970s (Shterev, 2022). These systems are now integral to the operations of many large enterprises, providing comprehensive solutions for managing business processes, data, and communications across various functions within an organization (Ahmed et al., 2023).

As SAP systems have grown in complexity and functionality, so too has the need for robust cybersecurity measures. Cybersecurity in the context of SAP systems encompasses a broad range of protocols and practices designed to protect data integrity, confidentiality, and availability (Chang et al., 2018). This is particularly crucial during system upgrades, which are often periods of heightened vulnerability due to the extensive changes being made to system architecture, software, and configurations (Chang et al., 2018).

The primary objective of this paper is to evaluate the effectiveness of cybersecurity protocols in SAP system upgrades from both an administrative and technical perspective. This involves examining the roles and responsibilities of administrators in ensuring security during upgrades, as well as the technical challenges and solutions associated with maintaining cybersecurity in SAP environments. By addressing both perspectives, the paper aims to provide a comprehensive understanding of the measures necessary to protect SAP systems against cyber threats during upgrades.

Administrators play a crucial role in the cybersecurity landscape of SAP system upgrades. Their responsibilities include planning and preparation, conducting risk assessments, and ensuring compliance with relevant regulations and standards (Majerník et al., 2023, Muhaimin, 2022). They are also tasked with managing user access and permissions, which is a critical aspect of maintaining system security. Effective administration involves continuous monitoring and auditing to detect and mitigate potential threats (Turken et al., 2023).

From a technical perspective, securing SAP systems during upgrades involves addressing challenges related to software updates, data protection, and system integration (Jinhong, 2024). Technical solutions such as encryption, data masking, and the implementation of advanced authentication mechanisms are essential for safeguarding sensitive information (Jinhong, 2024). Additionally, the use of intrusion detection systems (IDS) and other cybersecurity tools can help in detecting and responding to potential threats in real time (Chary et al., 2023).

The structure of this paper is organized into several key sections. The first section provides an overview of SAP systems, including their history and core functionalities. The second section delves into the various cybersecurity protocols relevant to SAP systems and the general best practices in cybersecurity. The third section examines the administrative perspective, highlighting the challenges and strategies for effective cybersecurity management during upgrades. The fourth section explores the technical perspective, discussing the technical aspects of SAP system upgrades and the solutions for enhancing cybersecurity. The fifth section presents case studies that illustrate successful and unsuccessful SAP system upgrades, providing insights into the lessons learned. The sixth section offers a comparative analysis of the administrative and technical perspectives, followed by a discussion of future trends and developments in cybersecurity for SAP systems. The paper concludes with a summary of key findings and recommendations for future research and practice.

II. OVERVIEW OF SAP SYSTEMS

The history of SAP systems dates back to the early 1970s when five former IBM employees in Mannheim, Germany, founded SAP SE (Holubiev et al., 2022). Initially named "Systemanalyse und Programmentwicklung" (System Analysis and Program Development), the company aimed to create standardized software for business solutions (Chinthamu and Karukuri, 2023). The first product, SAP R/1, was released in 1972 and focused on financial accounting. As businesses demanded more integrated solutions, SAP introduced SAP R/2 in 1979, which expanded functionalities to include materials management and production planning, operating on mainframes with a robust database (Holubiev et al., 2022).

The significant leap occurred in 1992 with the release of SAP R/3, which transitioned to a client-server architecture, making it more flexible and accessible (Aleksy and Korthaus, 1999). SAP R/3 incorporated modules for various business processes, such as sales and distribution, human resources, and asset management, establishing SAP as a leader in enterprise resource planning (ERP) software (Kemper et al., 1998). This evolution continued with SAP ECC (ERP Central Component) and eventually led to SAP S/4HANA in 2015. S/4HANA, built on the in-memory HANA database, offered real-time processing capabilities and simplified the data model, enabling faster analytics and transaction processing (Turken et al., 2023).

SAP systems are designed to support and integrate all facets of a business. The core functionalities of SAP systems include modules for financial accounting (FI), controlling (CO), sales and distribution (SD), materials management (MM), production planning (PP), and human resources (HR) (Lin et al., 2022). These modules facilitate the seamless flow of information across different business units, enhancing coordination and efficiency. For instance, the financial accounting module helps manage financial transactions and reporting (Škorić, 2021), while the materials management module supports procurement and inventory management (Lie and Ernestine, 2016).

SAP systems also incorporate advanced functionalities such as Business Information Warehouse (BW) for data warehousing and analytics (Turken et al., 2023; Kumar, 2023), and Customer Relationship Management (CRM) for managing customer interactions (Chandra and Yulistia, 2023; Li et al., 2023). These functionalities enable organizations to derive insights from their data and improve decision-making processes (Anshari and Retno, 2023; Chauhan, 2023). Additionally, SAP's integration technologies like Business Application Programming Interfaces (BAPIs) and Intermediate Documents (IDocs) facilitate interoperability with other systems, ensuring a cohesive IT environment (Efuntade and Efuntade, 2023; Chari et al., 2023).

Upgrading SAP systems is crucial for several reasons. First, it ensures that the software remains compatible with the latest technological advancements and industry standards. This compatibility is vital for maintaining system performance, security, and compliance. As cyber threats evolve, upgrading SAP systems helps incorporate the latest security features and protocols, thereby protecting sensitive business data from potential breaches (Chang et al., 2018).

Moreover, system upgrades often introduce new functionalities and enhancements that can significantly improve business processes (Laher et al., 2023). For example, the transition from SAP ECC to SAP S/4HANA involves moving to a more advanced database technology that offers real-time analytics and simplified data models (Poroca, 2023; Sirse et al., 2023). This transition can lead to more efficient data processing, reduced operational costs, and improved decision-making capabilities (Syauqie et al., 2023). Furthermore, regular upgrades are necessary to receive support and updates from SAP, ensuring that the system remains reliable and secure (Zeng et al., 2022). From an administrative perspective, upgrading SAP systems involves careful planning and execution. Administrators must conduct thorough risk assessments, ensure data integrity during the migration process, and provide adequate training for end-users to adapt to new functionalities. On the technical side, upgrades may require significant changes to the underlying infrastructure, including hardware updates, software patches, and modifications to custom-developed applications (Syauqie et al., 2023).

III. CYBERSECURITY PROTOCOLS IN SAP SYSTEMS

Cybersecurity protocols are essential frameworks and procedures that ensure the security of information systems, protecting data from unauthorized access, theft, and damage. These protocols are designed to safeguard the integrity, confidentiality, and availability of information, which are fundamental principles in cybersecurity (Shmeleva, 2020). The increasing volume and sophistication of cyber attacks highlight the importance of robust cybersecurity protocols to secure sensitive information and protect national security (KumarGoutam, 2015). Effective cybersecurity protocols are critical for preventing breaches that could lead to significant financial and reputational damage for organizations and individuals alike (Chopra et al., 2022).

The primary role of cybersecurity protocols is to create a secure environment for the storage, transmission, and processing of data. In the context of enterprise systems such as SAP, these protocols help maintain the integrity of business operations by ensuring that data remains accurate and unaltered during transactions and storage (Puthal et al., 2017). Additionally, cybersecurity protocols are vital for protecting intellectual property and personal information, which are increasingly targeted by cybercriminals. By implementing these protocols, organizations can safeguard their critical assets against a wide range of cyber threats (Sharma & Maurya, 2020).

Several types of cybersecurity protocols are relevant to SAP systems, each designed to address specific security concerns. One key protocol is encryption, which involves encoding data to prevent unauthorized access. Encryption is crucial for protecting data in transit and at rest, ensuring that even if data is intercepted, it cannot be read without the decryption key (Alonso et al., 2024). Another important protocol is the use of secure communication channels, such as Transport Layer Security (TLS), which encrypts data exchanged between users and systems to prevent eavesdropping and tampering (AbdulJabbar et al., 2013).

Access control mechanisms are also critical in SAP systems. These include the implementation of strong authentication methods, such as multi-factor authentication (MFA), which require users to provide multiple forms of verification before gaining access to sensitive systems. Access control protocols ensure that only authorized individuals can access specific data and functionalities within the SAP environment (Sipos, 2023). Additionally, network security protocols, such as firewalls and intrusion detection systems (IDS), are used to monitor and protect network traffic, preventing unauthorized access and identifying potential threats in real-time (Hussain et al., 2023).

General best practices in cybersecurity for enterprise systems include a combination of proactive and reactive measures to ensure comprehensive protection. One fundamental practice is regular software updates and patch management. Keeping software up to date is crucial for addressing vulnerabilities that could be exploited by attackers. This is especially important in complex systems like SAP, where outdated components can become significant security liabilities (KumarGoutam, 2015). Regular updates help to mitigate risks by ensuring that the latest security enhancements are applied (Shmeleva, 2020).

Another best practice is the implementation of comprehensive data protection strategies, including the use of backup and disaster recovery plans. These strategies ensure that data can be restored in the event of a cyber incident, minimizing downtime and data loss (Elkhannoubi & Belaïssaoui, 2015). Additionally, conducting regular security audits and vulnerability assessments can help identify and address potential weaknesses in the system before they can be exploited by attackers (Chang et al., 2018).

User education and awareness are also critical components of a robust cybersecurity strategy. Training employees on best practices for cybersecurity, such as recognizing phishing attempts and using strong, unique passwords, can significantly reduce the risk of human error leading to security breaches (Chopra et al., 2022). Furthermore, developing a cybersecurity culture within the organization can promote proactive security behaviors and ensure that cybersecurity is considered a priority at all levels of the organization (Ghernouti-Hélie, 2010).

IV. ADMINISTRATIVE PERSPECTIVE

4.1 Role of Administrators in SAP System Upgrades

Administrators play a pivotal role in SAP system upgrades, ensuring that the complex process of upgrading enterprise resource planning (ERP) systems is executed smoothly and efficiently. Their responsibilities encompass planning and preparation, risk assessment, and stakeholder communication, each of which is critical to the success of the upgrade project.

Planning and preparation are foundational tasks in any SAP system upgrade. Administrators must develop a comprehensive project plan that outlines the objectives, scope, timeline, and resources required for the upgrade (Firdaus et al., 2023). This involves coordinating with various departments to gather requirements and ensure that the upgrade aligns with the organization's overall strategic goals (Bopalia, 2023). Effective planning helps mitigate potential disruptions to business operations, which can be significant during system upgrades (Christiandava et al., 2023).

Administrators also need to become proficient in using SAP's specific upgrade tools for both ABAP and Java systems. These tools facilitate the technical aspects of the upgrade, such as data migration, system configuration, and performance tuning (Sofjan et al., 2023). A deep understanding of these tools and the upgrade process is essential for troubleshooting and resolving issues that may arise during the upgrade. This technical expertise enables administrators to make informed decisions and implement best practices, ensuring that the upgrade is performed efficiently and with minimal risk (Sofjan et al., 2023). Risk assessment is another critical component of the administrator's role. During an SAP system upgrade, various risks can threaten the project's success, including data loss, system downtime, and security vulnerabilities (Lim et al., 2023; Raazi et al., 2023). Administrators must conduct thorough risk assessments to identify potential threats and develop strategies to mitigate them. This involves evaluating the current system's vulnerabilities, testing the

upgrade in a controlled environment, and planning for disaster recovery scenarios (Kalouptsoglou et al., 2022). By proactively addressing these risks, administrators can minimize the likelihood of encountering severe issues during the actual upgrade.
One of the key tasks in risk assessment is ensuring data integrity and security (Mangaoang and Monreal, 2024). Administrators must verify that all data is accurately transferred and remains secure throughout the upgrade process. This includes implementing robust backup procedures, encryption protocols, and access controls to protect sensitive information (Pal et al., 2024; Phatangare, 2024). Additionally, administrators need to monitor the system for any anomalies or unauthorized access attempts, ensuring that any potential security breaches are quickly identified and addressed (Sahu et al., 2024; Fayayola et al., 2024).

Stakeholder communication is crucial for the success of an SAP system upgrade. Administrators must communicate effectively with various stakeholders, including executives, department heads, IT staff, and end-users (Andisty and Harmain, 2022). This involves keeping stakeholders informed about the project's progress, potential impacts on business operations, and any changes to the project plan (Syauqie et al., 2023). Clear and consistent communication helps manage expectations and ensures that all parties are prepared for the upgrade (Damm et al., 2022).

Administrators also play a key role in training and supporting end-users (Seneviratne and Colombage, 2023. After the upgrade, users need to understand how to operate the new system effectively. Administrators must develop and deliver training programs to ensure that users are comfortable with the new features and functionalities. This training is essential for minimizing disruptions to business operations and ensuring that the organization can fully leverage the benefits of the upgraded system (Ketoma et al., 2023). In addition to training, administrators must provide ongoing support to address any issues that arise post-upgrade (Liu et al., 2022). This includes troubleshooting technical problems, answering user questions, and making necessary adjustments to system configurations (Wang, 2022; Azevedo et al., 2023). Effective post-upgrade support is critical for maintaining user satisfaction and ensuring that the upgraded system operates smoothly (Zhao et al., 2022).

4.2 Cybersecurity Challenges Faced by Administrators

Administrators face significant cybersecurity challenges when managing SAP system upgrades, as these upgrades involve complex processes and substantial changes to the system's architecture. Among these challenges, identifying potential vulnerabilities, managing user access and permissions, and ensuring compliance with regulations are paramount.

Identifying potential vulnerabilities is a critical task for administrators during SAP system upgrades (Martinez et al., 2023). Vulnerabilities can arise from software bugs, configuration defects, or flaws in the system's design (Bojanova et al., 2023; Patel et al., 2023). These weaknesses can be exploited by malicious actors to gain unauthorized access or disrupt business operations (Chadha et al., 2022).Effective identification of these vulnerabilities involves conducting thorough assessments of the system's current state, including code reviews, configuration checks, and security audits. Tools like the J48 decision tree algorithm can aid in predicting software vulnerabilities and enhancing system security (Murthy and Shilpa, 2021). Ethical hacking techniques, such as penetration testing using tools like Nmap and Nessus, are also instrumental in uncovering vulnerabilities. These methods simulate real-world attacks to identify security gaps that need to be addressed (Berger & Jones, 2016).

In addition to technical assessments, administrators must remain vigilant to emerging threats and continuously update their knowledge and strategies. This involves staying informed about the latest cybersecurity trends and incorporating advanced technologies, such as machine learning and artificial intelligence, to predict and mitigate vulnerabilities (Ghazal et al., 2022). By leveraging these technologies, administrators can develop more robust defenses against sophisticated cyber threats.

Managing user access and permissions is another significant challenge in SAP system upgrades. Proper access control ensures that only authorized personnel

can access sensitive information and critical system functionalities. This is crucial for preventing unauthorized access and potential data breaches. Administrators must implement stringent access control mechanisms, including multi-factor authentication (MFA) and role-based access control (RBAC), to enforce security policies effectively (Chang et al., 2018).

Administrators need to regularly review and update user permissions to reflect changes in roles and responsibilities (Baugher and Qu, 2024). This process involves conducting periodic audits to ensure that access rights are aligned with current job functions and removing access for users who no longer require it. Automated tools can assist in monitoring and managing user access, providing real-time alerts for any unauthorized access attempts or unusual activities (Tan et al., 2024). Additionally, administrators should educate users about the importance of cybersecurity practices, such as creating strong passwords and recognizing phishing attempts, to minimize the risk of human error leading to security breaches (Oladokun et al., 2024; Rama and Keevy, 2023).

Ensuring compliance with regulations is a critical aspect of cybersecurity management during SAP system upgrades. Organizations must adhere to various regulatory requirements and standards to protect sensitive data and maintain legal and industry compliance. Regulations such as the General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), and Sarbanes-Oxley Act (SOX) impose strict guidelines on data security and privacy (Yusif & Hafeez-Baig, 2021).

Administrators must ensure that the upgraded SAP system complies with these regulations by implementing necessary controls and safeguards. This includes encrypting sensitive data, maintaining detailed audit logs, and ensuring secure data transmission and storage. Regular compliance audits and assessments are essential to verify that the system meets all regulatory requirements. Additionally, administrators should stay informed about changes in regulations and update security practices accordingly to maintain compliance (Bhakare et al., 2023).

4.3 Strategies for Effective Cybersecurity Management During Upgrades

Effective cybersecurity management during SAP system upgrades requires a comprehensive approach that includes regular training and awareness programs, incident response planning, and continuous monitoring and auditing. Each of these strategies plays a crucial role in ensuring the security and integrity of the system throughout the upgrade process.

Regular training and awareness programs are fundamental to maintaining a high level of cybersecurity. These programs educate employees about the latest cyber threats, security policies, and best practices for protecting sensitive information. Given the rapidly evolving nature of cyber threats, ongoing training ensures that employees remain vigilant and capable of identifying and responding to potential security incidents (Cheng & Wang, 2022). By fostering a culture of cybersecurity awareness, organizations can significantly reduce the risk of human error, which is often a primary cause of security breaches.

Training programs should cover various aspects of cybersecurity, including the importance of strong passwords, recognizing phishing attempts, and the proper use of security tools. Additionally, specialized training for IT staff and administrators on the specific security features and protocols of the SAP system can enhance their ability to manage and secure the system effectively. Hands-on workshops and simulations of cyber attacks can also be valuable in helping employees understand real-world scenarios and how to respond appropriately (Wallen, 2022).

Incident response planning is another critical component of cybersecurity management during SAP system upgrades. An incident response plan outlines the steps to be taken in the event of a security breach or other cyber incident. This plan should include procedures for identifying and containing the incident, assessing the impact, and implementing recovery measures to restore normal operations (Möller & Vakilzadian, 2023). A well-developed incident response plan ensures that organizations can respond quickly and effectively to minimize damage and prevent further attacks.

Key elements of an incident response plan include defining roles and responsibilities, establishing communication protocols, and maintaining an updated list of contacts for internal and external stakeholders. Regular drills and simulations can help test the effectiveness of the plan and ensure that all team members are familiar with their roles and the procedures to follow during an incident (Vinnakota, 2016). Additionally, documenting and analyzing incidents can provide valuable insights into vulnerabilities and inform future security measures.

Continuous monitoring and auditing are essential for maintaining the security of an SAP system during and after an upgrade. Continuous monitoring involves the real-time tracking of network activity, system performance, and user behavior to detect anomalies that may indicate a security threat. Advanced monitoring tools, such as Security Information and Event Management (SIEM) systems, can aggregate and analyze data from multiple sources to provide a comprehensive view of the system's security posture (Bitmanov & Uruzbaeva, 2021).

Regular audits complement continuous monitoring by providing a thorough evaluation of the system's security controls, configurations, and compliance with regulatory requirements. Audits can identify gaps in security policies, procedures, and technologies, enabling organizations to address vulnerabilities proactively. Both internal and external audits are crucial for ensuring that the system remains secure and that any weaknesses are promptly identified and mitigated (Škanata, 2020).

Effective auditing also involves the use of automated tools to streamline the process and improve accuracy. These tools can help administrators track changes in system configurations, monitor access controls, and ensure that security patches are applied promptly. By continuously evaluating and improving their security measures, organizations can stay ahead of potential threats and maintain a robust defense against cyber attacks (Galinec & Steingartner, 2017).

V. TECHNICAL PERSPECTIVE

5.1 Technical Aspects of SAP System Upgrades

SAP system upgrades are complex endeavors involving various technical aspects, such as software updates, patches, system integration, and compatibility. These elements are crucial for maintaining the system's functionality, security, and performance. Effective management of these technical aspects ensures a smooth transition to the upgraded system and minimizes disruptions to business operations.

Software updates and patches are fundamental components of SAP system upgrades. These updates typically include enhancements to system functionality, security improvements, and bug fixes (Farhi et al., 2023). Regular software updates are essential for addressing vulnerabilities that could be exploited by cyber attackers (Shen et al., 2023). Comprehensive planning and execution are required to ensure successful implementation of these updates (Williams et al., 2023). This involves understanding the specific requirements of the system, testing the updates in a controlled environment, and ensuring that all dependencies are addressed before deploying the updates to the production environment (Xiao et al., 2023).

Patching is another critical aspect of maintaining the security and stability of SAP systems. Patches are often released in response to identified vulnerabilities or performance issues. Administrators must stay informed about available patches and apply them promptly to protect the system from potential threats. Effective patch management involves creating a schedule for regular patch application, testing patches thoroughly to ensure they do not introduce new issues, and monitoring the system after patch deployment to verify that the patches have been applied successfully and that the system operates as expected (Haryadi et al., 2022).

System integration and compatibility are equally important in the context of SAP system upgrades. Integration ensures that the SAP system can effectively communicate and interact with other software and hardware components within the organization's IT infrastructure (Xue and Dong, 2023; Tripathy et al., 2022). This is particularly important for businesses that rely on multiple interconnected systems to support their operations (Poroca, 2023).

Compatibility, on the other hand, ensures that the upgraded system can work seamlessly with existing applications and devices (Wang et al., 2022).

One of the primary challenges in system integration is ensuring that data flows smoothly between the SAP system and other systems. This requires a thorough understanding of the data structures and communication protocols used by different systems (Berdie et al., 2022). Administrators must map data fields accurately and establish reliable data exchange mechanisms to prevent data loss or corruption during the upgrade process.

Compatibility issues can arise when there are significant differences between the versions of the SAP system and the other systems with which it interacts (Liu et al., 2022). For instance, new features or changes in the data structure of the upgraded SAP system may not be supported by older versions of other systems (Zhao et al., 2022). To address this, administrators must conduct compatibility testing to identify and resolve any issues before the upgrade is deployed. This may involve updating or modifying other systems to ensure they are compatible with the new version of the SAP system (Vitale et al., 2017).

In addition to these technical considerations, administrators must also ensure that the upgrade process itself is well-managed (Myronenko, 2023). This includes creating detailed project plans that outline the steps involved in the upgrade, assigning responsibilities to team members, and establishing timelines for each phase of the project (Wang et al., 2023). Effective project management helps to coordinate activities, track progress, and address any issues that arise promptly (Thant and Tin, 2023). Moreover, communication is key to successful system upgrades. Administrators must keep stakeholders informed about the upgrade process, potential impacts on business operations, and the benefits of the new system. This helps to manage expectations and ensure that all parties are prepared for the changes that will occur (Syauqie et al., 2023)

5.2 Cybersecurity Challenges in the Technical Domain
In the technical domain of SAP system upgrades, addressing cybersecurity challenges is paramount to ensuring the protection of data integrity and confidentiality, securing system interfaces and APIs, and mitigating threats from external sources. Each of these areas presents unique challenges that require targeted strategies and solutions to manage effectively. Protecting data integrity and confidentiality is a core aspect of cybersecurity in SAP systems (Nwobodo et al., 2024). Data integrity ensures that information remains accurate and unaltered during transmission and storage (Watney, 2024), while data confidentiality ensures that sensitive information is accessible only to authorized users (Abrahams et al., 2023). One of the primary challenges in this area is the potential for software bugs, configuration defects, and design flaws, which can create vulnerabilities that attackers might exploit (Riyadi et al., 2022). Regular updates and patches are essential to address these vulnerabilities promptly. Furthermore, the use of advanced encryption methods to protect data at rest and in transit is crucial. Encryption ensures that even if data is intercepted, it remains unreadable without the correct decryption key, thus maintaining its confidentiality (Chang et al., 2018).

Moreover, implementing stringent access control measures is critical for protecting data integrity and confidentiality. Multi-factor authentication (MFA) and role-based access control (RBAC) help ensure that only authorized personnel can access sensitive data. These measures, combined with regular auditing and monitoring of access logs, can significantly reduce the risk of unauthorized access and data breaches (Yusif & Hafeez-Baig, 2021).

Securing system interfaces and APIs is another significant challenge in the technical domain of SAP system upgrades (Chatterjee and Prinz, 2022). APIs, which enable different software applications to communicate with each other, are often targeted by attackers seeking to exploit vulnerabilities for unauthorized access or data manipulation (Tyllis et al., 2023). To secure these interfaces, it is essential to implement robust API security measures, such as authentication, authorization, and input validation (More et al., 2024). Ensuring that APIs adhere to security best practices, including the use of secure communication protocols like HTTPS, helps protect against common threats such as injection attacks and cross-site scripting (XSS) (Ghazal et al., 2022).

Additionally, regular security testing of APIs, including penetration testing and vulnerability scanning, can identify potential weaknesses before they can be exploited by attackers. Automated tools can be used to continuously monitor API activity, detecting and responding to suspicious behavior in real-time. This proactive approach to API security helps maintain the integrity and availability of the SAP system's interfaces (Alharbi et al., 2021).

Mitigating threats from external sources is a broad and ongoing challenge in cybersecurity. External threats, including malware, phishing attacks, and distributed denial-of-service (DDoS) attacks, can significantly disrupt SAP system operations if not adequately addressed (Jony and Hamim, 2024; Umoga et al., 2024). To mitigate these threats, a multi-layered security approach is necessary. This includes deploying firewalls, intrusion detection and prevention systems (IDPS), and anti-malware solutions to create a robust defense against external attacks (Qammar et al., 2023). Firewalls control incoming and outgoing network traffic based on predetermined security rules, while IDPS monitors network traffic for signs of malicious activity and takes action to prevent or mitigate attacks (Sharma et al., 2024; Al-Fawa'reh et al., 2024).

Moreover, leveraging artificial intelligence (AI) and machine learning (ML) technologies can enhance the ability to detect and respond to threats (Elbes et al., 2023). AI and ML can analyze vast amounts of data to identify patterns and anomalies that may indicate a security threat (Sirse et al., 2023). These technologies can also automate responses to detected threats, reducing the time it takes to mitigate potential attacks (Hasan et al., 2023). For example, AI-powered security tools like Darktrace and IBM QRadar can provide real-time threat detection and automated incident response, enhancing the overall security posture of SAP systems (Haripriya, Jolly and Venkadesh, 2023).

5.3 Technical Solutions for Enhancing Cybersecurity

Enhancing cybersecurity in SAP systems requires a multifaceted approach that integrates various technical solutions to protect sensitive data and ensure the integrity and security of the entire system (Mathieu and Turovlin, 2023). Key strategies include the use of encryption and data masking, the implementation of firewalls and intrusion detection systems, and the deployment of advanced authentication mechanisms. Each of these techniques addresses specific vulnerabilities and enhances the overall security posture of SAP systems. Encryption and data masking are critical for protecting sensitive data both in transit and at rest (Hisbullah et al., 2023).

Encryption involves converting data into a coded format that can only be deciphered with the correct decryption key (Sangewar and Gugulothu, 2023). This ensures that even if data is intercepted, it remains unreadable to unauthorized users. Data masking, on the other hand, involves modifying data to obscure sensitive information, making it unusable for unauthorized users while maintaining its utility for legitimate purposes (Jarwal et al., 2023). These techniques are essential for safeguarding personal and financial information, intellectual property, and other sensitive data stored in SAP systems.

Implementing encryption requires careful management of encryption keys and the selection of robust encryption algorithms (Jain and Kumar, 2023). For instance, Advanced Encryption Standard (AES) is widely used due to its strength and efficiency (Sri et al., 2023). Data masking can be applied dynamically during data access or statically in stored datasets, depending on the specific needs of the organization (Neetha et al., 2023).Both techniques help ensure compliance with regulatory requirements such as GDPR and HIPAA, which mandate the protection of personal data (Chang et al., 2018).

The implementation of firewalls and intrusion detection systems (IDS) is another vital component of enhancing cybersecurity in SAP systems (Akhiruddin and Sutabri, 2023). Firewalls act as a barrier between trusted internal networks and untrusted external networks, controlling incoming and outgoing traffic based on predetermined security rules (Teja et al., 2023). They prevent unauthorized access to the network and protect against a variety of cyber threats, including malware and denial-of-service (DoS) attacks (Fakiha, 2022). Intrusion detection systems monitor network traffic for suspicious activities and alert administrators to potential security breaches. IDS can be signature-based, which detects known threats, or

anomaly-based, which identifies unusual patterns that may indicate an attack (Alsunbul et al., 2016).

Combining firewalls and IDS provides a robust defense against cyber-attacks (Ramli and Alifsyah, 2023). Firewalls block unauthorized access (Qian, 2023), while IDS detect and respond to potential intrusions (Shrivastava and Yadav, 2023). Advanced IDS solutions incorporate machine learning and artificial intelligence to improve threat detection and reduce false positives (Xuan and Manohar, 2023). These systems can analyze vast amounts of data in real-time, identifying patterns and anomalies that may indicate a security threat (Larriva-Novo et al., 2023). By continuously updating their threat databases and learning from new attack patterns, these systems provide proactive security measures to protect SAP systems (Lourens et al., 2022).

Advanced authentication mechanisms are essential for ensuring that only authorized users can access sensitive information and critical system functions (González-Muñoz et al., 2023). Traditional password-based authentication is often insufficient due to the risk of password theft or reuse (Sadat et al., 2023). Multi-factor authentication (MFA) enhances security by requiring users to provide multiple forms of verification, such as something they know (password), something they have (security token), and something they are (biometric data) (Abdulkareem et al., 2023; Corona et al., 2023).MFA significantly reduces the risk of unauthorized access by making it more difficult for attackers to compromise all required factors (Ghazal et al., 2022).

In addition to MFA, advanced authentication mechanisms can include the use of single sign-on (SSO) solutions (Maidine and El-Yahyaoui, 2023), which allow users to authenticate once and gain access to multiple applications without needing to re-enter credentials (Guo et al., 2022). This improves user convenience and reduces the risk of credential fatigue, where users resort to insecure practices such as writing down passwords (Fauzi et al., 2023). Furthermore, the use of biometric authentication, such as fingerprint or facial recognition, provides an additional layer of security that is difficult for attackers to replicate (Dangi et al., 2023).

VI. CASE STUDIES

6.1 Case Studies of Successful SAP System Upgrade with Robust Cybersecurity

Successful SAP system upgrades with robust cybersecurity have become essential for organizations to enhance operational efficiency and protect sensitive data. A notable case is the Kenya Pipeline Company's (KPC) SAP IS-OIL software upgrade project. This upgrade focused on enhancing system functionalities to support oil and gas operations (Gichuru and Onjure, 2019). A critical factor in the project's success was the engagement of stakeholders during the project identification phase. This engagement ensured that the project team had the confidence and commitment necessary to mitigate risks, particularly those related to project ownership and accountability (Gichuru and Onjure, 2019). The study on this project underscores the importance of stakeholder involvement in achieving successful outcomes and highlights how their engagement practices directly influenced project performance (Gichuru and Onjure, 2019).

In another significant case, Petroleum Development Oman (PDO) embarked on an extensive SAP system upgrade to transition from a legacy Well Management System (WMS) to a NextGen system (Shekaili et al., 2023). This upgrade spanned multiple assets and aimed to improve operational excellence, health and safety, and cybersecurity, while also reducing the carbon footprint. The project was successful due to a comprehensive approach that included rigorous testing, training, and the integration of advanced cybersecurity measures (Shekaili et al., 2023). These measures were crucial in protecting the upgraded system from potential cyber threats, thereby ensuring the integrity and availability of critical data and operations (Shekaili et al., 2023).

Cybersecurity was a central theme in these upgrades, as illustrated by the measures taken to secure the new systems. For example, in PDO's case, the transition to the NextGen system involved the implementation of state-of-the-art cybersecurity protocols. These protocols included multi-factor authentication, regular security audits, and real-time monitoring of system activities to detect and respond to any suspicious behavior promptly (Shekaili et al., 2023). Such measures are vital in preventing unauthorized access

and protecting sensitive operational data from cyberattacks.

The successful upgrades also highlight the role of continuous improvement and adaptation in maintaining robust cybersecurity (Gichuru and Onjure, 2019; Shekaili et al., 2023). Organizations must stay abreast of the latest cybersecurity trends and threats, continuously updating their security measures to address new vulnerabilities. This proactive approach was evident in PDO's project, where the team regularly reviewed and updated their cybersecurity strategies to align with the latest industry standards and best practices (Shekaili et al., 2023).

Furthermore, the integration of artificial intelligence (AI) and machine learning (ML) in cybersecurity frameworks has shown promising results. AI and ML technologies can analyze vast amounts of data to identify patterns and anomalies that may indicate potential security threats (Donepudi, 2015). The adoption of these technologies in SAP system upgrades provides an additional layer of protection, enhancing the system's ability to detect and respond to cyber threats in real-time (Donepudi, 2015).

6.2 Case Studies of SAP System Upgrade with Cybersecurity Breaches

Upgrading SAP systems, crucial for maintaining business efficiency and ensuring the integration of modern functionalities, poses significant cybersecurity challenges. One notable case study involves a significant breach during the upgrade of an SAP system utilizing the Orion tool (Akhtar, 2021). This breach was part of the larger SolarWinds hacking attack, which exposed vulnerabilities within the SAP systems. Hackers were able to introduce malicious code during the upgrade process, leading to unauthorized access to various clients' systems (Akhtar, 2021). This incident underscored the heightened threat landscape in the post-SolarWinds era, revealing how even trusted software upgrades could be compromised to serve as vectors for cyber attacks (Akhtar, 2021).

A similar scenario is illustrated in a case study focusing on the role of leadership in cybersecurity risk management (Falco and Rosenbach, 2021).. The study of the Equifax breach demonstrates the importance of strong leadership and accountability in preventing and mitigating cybersecurity risks (Falco and Rosenbach, 2021). The Equifax case, while not directly involving SAP, underscores the broader implications of leadership in managing cybersecurity during system upgrades, emphasizing the need for a robust cybersecurity culture within organizations (Falco and Rosenbach, 2021).

In another instance, the analysis of security vulnerabilities and forensic investigation techniques in ROS2-based applications showcases the potential risks during system upgrades. This case study highlights issues such as unauthorized data injection and access, and denial of service attacks, illustrating how these vulnerabilities can be exploited during system upgrades (Patel et al., 2022). The findings underscore the need for comprehensive security assessments and forensic capabilities to identify and mitigate risks effectively (Patel et al., 2022).

The challenges of AI-based cybersecurity during system upgrades are explored in a study that examines the roles and hurdles of AI in various phases of cybersecurity, including prevention, detection, and response. This case study highlights the potential of AI to enhance security measures during system upgrades by providing automated assessments of security vulnerabilities (Alalwan, 2022). However, it also points out significant challenges such as regulatory compliance, trust, and financial costs that must be addressed to leverage AI effectively in cybersecurity (Alalwan, 2022).

Moreover, human error remains a critical factor in cybersecurity breaches during SAP system upgrades. A study investigating the impact of cybersecurity education, training, and awareness on minimizing human errors reveals that a significant number of breaches result from lapses in human judgment (Amoresano and Yankson, 2023). The study underscores the importance of continuous training and awareness programs to equip employees with the knowledge and skills needed to identify and respond to potential threats during system upgrades (Amoresano and Yankson, 2023).

These case studies collectively highlight the multifaceted nature of cybersecurity challenges during SAP system upgrades. They emphasize the need for a comprehensive approach that includes strong leadership, advanced technological solutions such as AI, robust security protocols, and continuous human training and awareness (Akhtar, 2021; Falco and Rosenbach, 2021; Alalwan, 2022; Patel et al., 2022; Amoresano and Yankson, 2023). By addressing these various aspects, organizations can better safeguard their systems against breaches during critical upgrade processes.

VII. COMPARISON OF ADMINISTRATIVE AND TECHNICAL PERSPECTIVES

The comparative analysis of administrative and technical perspectives in SAP system upgrades reveals the diverse but complementary roles these two domains play in ensuring the success and security of system enhancements. Both perspectives are integral to managing the complexities and challenges associated with SAP upgrades, yet they approach these tasks from different angles, focusing on unique aspects that collectively contribute to the overall success of the upgrade process.

From the administrative perspective, the focus is on strategic planning, risk management, and stakeholder communication (Hanafi et al., 2023). Administrators are responsible for ensuring that the upgrade aligns with the organization's strategic goals and regulatory requirements. This involves detailed planning and coordination across various departments to gather requirements, allocate resources, and establish timelines. Effective risk management is crucial in this domain, where administrators must identify potential risks, such as data breaches or system downtimes, and develop mitigation strategies to address them (Domagała et al., 2021). Additionally, clear and consistent communication with stakeholders is essential to manage expectations, provide updates on the upgrade progress, and address any concerns that may arise during the process.

In contrast, the technical perspective centers on the practical implementation of the upgrade, focusing on aspects such as software updates, data migration, system integration, and cybersecurity (Munjala, 2024). Technicians and IT specialists are tasked with the hands-on execution of the upgrade, ensuring that the new system components are compatible with existing infrastructure and that data is accurately migrated without loss or corruption. Cybersecurity is a critical concern from the technical standpoint, where measures such as encryption, data masking, firewalls, and intrusion detection systems are implemented to protect the system from potential threats (Poroca, 2023).

A common challenge in SAP system upgrades is the need to balance the strategic goals of the organization with the technical feasibility of the upgrade (Sirse et al., 2023; Momani et al., 2023). Administrators may push for ambitious timelines and extensive functionality enhancements, while technicians may caution against the potential risks and complexities involved (Amalberti et al., 2022). Effective collaboration between these two perspectives is essential to develop a realistic and achievable upgrade plan that meets organizational goals without compromising system security and stability (Syauqie et al., 2023).

One of the critical issues that both perspectives must address is the integration of robust cybersecurity measures. The administrative perspective emphasizes the need for compliance with regulatory standards and the protection of sensitive data, while the technical perspective focuses on the implementation of specific security technologies and protocols. A holistic approach that combines these viewpoints ensures that the upgrade is both compliant and secure, mitigating the risk of cyber threats (Domagała et al., 2021).

Another shared challenge is the management of user access and permissions. Administrators are concerned with defining and enforcing access policies that align with organizational roles and responsibilities (Fan et al., 2022). Technicians, on the other hand, implement these policies through technical means, such as multi-factor authentication (Xu et al., 2023; Papaspirou et al., 2023) and role-based access control (Yuan et al., 2023). Effective management of user access is crucial to prevent unauthorized access and ensure that users have the necessary permissions to perform their tasks without compromising system security (Prajwal and Deepak, 2023).

Continuous monitoring and auditing are also essential activities that bridge the administrative and technical domains (Raj, 2024). Administrators establish policies for regular audits and monitoring to ensure compliance and identify potential issues early (Supit and Irwansyah, 2024). Technicians execute these audits, using advanced tools and technologies to monitor system activity, detect anomalies, and respond to incidents (Zelmati et al., 2023). This ongoing vigilance helps maintain the integrity and security of the SAP system, ensuring that it operates effectively and securely post-upgrade.

VIII. RECOMMENDATIONS

A holistic approach to cybersecurity in SAP upgrades is essential to ensure the security, compliance, and efficiency of the system. This approach integrates administrative, technical, and operational measures, creating a comprehensive defense strategy that addresses various aspects of cybersecurity. First and foremost, conducting thorough risk assessments is crucial. These assessments identify potential vulnerabilities and the impacts of cyber threats, enabling organizations to develop targeted mitigation strategies (Kedarya & Elalouf, 2023).

Administratively, it is imperative to establish clear cybersecurity policies and procedures that align with regulatory requirements and industry best practices. These policies should include guidelines for data protection, access control, incident response, and regular audits. Ensuring compliance with standards such as GDPR, HIPAA, and ISO/IEC 27001 helps protect sensitive information and maintain trust with stakeholders (Domagała et al., 2021).

From a technical perspective, implementing advanced security technologies such as encryption, multi-factor authentication, and intrusion detection systems is vital. Encryption protects data both at rest and in transit, ensuring that it remains confidential and secure. Multi-factor authentication adds an extra layer of security, making it more difficult for unauthorized users to access the system. Intrusion detection systems monitor network activity in real-time, identifying and responding to potential security incidents promptly (Chang et al., 2018).

Operationally, continuous monitoring and regular security audits are essential to maintain a robust cybersecurity posture. Monitoring tools help detect anomalies and potential threats early, allowing for swift response and mitigation. Regular security audits assess the effectiveness of existing security measures and identify areas for improvement, ensuring that the system remains secure against evolving threats (Kedarya & Elalouf, 2023).

Training and awareness programs for employees are also crucial components of a holistic approach. Educating staff about cybersecurity risks and best practices helps create a security-conscious culture within the organization, reducing the likelihood of successful social engineering attacks and human error-related breaches (Domagała et al., 2021).

IX. FUTURE TRENDS AND DEVELOPMENTS

Emerging threats in cybersecurity for SAP systems are continuously evolving, driven by the increasing sophistication of cyber-attacks and the expanding digital landscape. One significant emerging threat is the rise of advanced persistent threats (APTs), which are long-term, targeted attacks aimed at stealing sensitive information or disrupting operations. These threats are often state-sponsored and utilize a combination of social engineering, zero-day exploits, and malware to infiltrate systems undetected (Jerbi, 2023). The proliferation of Internet of Things (IoT) devices also broadens the attack surface, providing new entry points for cybercriminals to exploit (Li et al., 2020). Additionally, ransomware attacks have become more prevalent and sophisticated, targeting critical infrastructure and demanding high ransom payments to restore data access (Kante et al., 2024; Khaliq et al., 2024).

Future advancements in cybersecurity protocols are essential to counter these emerging threats effectively. One promising development is the shift towards hardware-level security solutions. These solutions integrate security features directly into hardware components, providing a more robust defense against tampering and unauthorized access. This approach is particularly relevant for SAP systems, which handle sensitive business data and require high levels of security (Chan et al., 2018). Another significant

advancement is the use of quantum-safe encryption algorithms. As quantum computing becomes more accessible, traditional encryption methods will become vulnerable. Quantum-safe encryption provides a means to protect data against the computational power of quantum computers, ensuring long-term data security (Hummelholm, 2023).

The role of artificial intelligence (AI) and machine learning (ML) in enhancing cybersecurity is becoming increasingly crucial. AI and ML can analyze vast amounts of data to detect patterns and anomalies indicative of cyber threats. These technologies enable predictive threat modeling, which can identify potential attacks before they occur, allowing for proactive defense measures (Alghamdi, 2020). For instance, AI-powered intrusion detection systems can monitor network traffic in real-time, recognizing and responding to suspicious activities more efficiently than traditional methods. Machine learning algorithms can also improve the accuracy of threat detection by learning from historical attack data and adapting to new threat vectors (Sasikala & Sharma, 2022).

AI and ML also enhance incident response capabilities. Automated response systems can be programmed to execute predefined actions when a threat is detected, such as isolating affected systems or initiating data backup procedures. This reduces response times and minimizes the impact of cyber incidents. Furthermore, AI-driven analytics can provide insights into attack patterns and root causes, helping organizations improve their cybersecurity posture and prevent future attacks (Li et al., 2020).

Despite the advancements in AI and ML, there are challenges to their implementation. One significant challenge is the need for large datasets to train machine learning models effectively. These datasets must be comprehensive and accurately labeled to ensure the models can learn to detect a wide range of threats (Pan et al., 2023; Khalid et al., 2023). Additionally, there is the risk of adversarial attacks, where attackers manipulate AI models to evade detection. To mitigate these risks, organizations must implement robust data management practices and continuously update their AI models to adapt to new threats (Sasikala & Sharma, 2022).

CONCLUSION

This paper has comprehensively explored the multifaceted aspects of cybersecurity in SAP system upgrades, emphasizing both administrative and technical perspectives. The key findings underscore the critical importance of robust planning, risk assessment, and continuous monitoring to ensure the security and efficiency of SAP system upgrades. From the administrative viewpoint, effective stakeholder communication, comprehensive training programs, and adherence to regulatory standards are essential. The technical perspective highlights the necessity of implementing advanced security measures such as encryption, multi-factor authentication, and intrusion detection systems.

The analysis reveals that cybersecurity challenges in SAP upgrades are significant and evolving. Administrators must balance strategic goals with technical feasibility, ensuring that upgrades do not compromise security. The integration of robust cybersecurity measures into the upgrade process is not just beneficial but essential to protect against the increasingly sophisticated cyber threats. This involves a proactive approach to identifying vulnerabilities, managing user access, and ensuring compliance with regulatory requirements.

The importance of effective cybersecurity in SAP system upgrades cannot be overstated. As businesses increasingly rely on SAP systems for critical operations, the potential impact of cybersecurity breaches grows. Effective cybersecurity measures protect not only sensitive data but also the integrity and availability of business processes. A breach during an upgrade can have far-reaching consequences, including financial loss, reputational damage, and regulatory penalties. Therefore, integrating comprehensive cybersecurity strategies into the upgrade process is crucial for safeguarding business continuity and maintaining stakeholder trust.

Looking forward, future research and practice should focus on several key areas. Firstly, there is a need for continuous development and refinement of cybersecurity protocols to keep pace with emerging threats. This includes exploring new technologies such as quantum-safe encryption and AI-driven security

solutions. Secondly, there should be an emphasis on developing integrated security frameworks that combine administrative policies with technical measures, ensuring a holistic approach to cybersecurity. Finally, ongoing training and awareness programs for employees at all levels are vital to maintaining a security-conscious culture within organizations.

Hence, the successful upgrade of SAP systems hinges on a comprehensive approach to cybersecurity that integrates both administrative and technical perspectives. By prioritizing security at every stage of the upgrade process, organizations can protect their critical systems from cyber threats and ensure the continued efficiency and reliability of their SAP environments. Future advancements in cybersecurity technologies and practices will be crucial in addressing the ever-evolving landscape of cyber threats, and ongoing research will play a key role in shaping these developments.

REFERENCES

[1] AbdulJabbar, M.A., Sagheer, A.M. and Abdulhameed, A.A. (2013) "Transport Layer Security Protocol for Intranet," *International Journal of Computer Applications*, 81(1), pp. 22–26. Available at: https://doi.org/10.5120/13976-1971.

[2] Abdulkareem, M.I., Ashour, O.I. and Salman, Y.B. (2023) "Secure IoT Entrance Using Mobile Application." Available at: https://doi.org/10.1109/emcturkiye59424.2023.10287534.

[3] Abrahams, N.T.O., Ewuga, N.S.K., Kaggwa, N.S., Uwaoma, N.P.U., Hassan, N.A.O. and Dawodu, N.S.O. (2023) "Review of strategic alignment: Accounting and cybersecurity for data confidentiality and financial security," *World Journal of Advanced Research and Reviews*, 20(3), pp. 1743–1756. Available at: https://doi.org/10.30574/wjarr.2023.20.3.2691.

[4] Ahmed, A., Awais, M., Siraj, M. and Umar, M. (2023) "Enhancing Cybersecurity with Trust-Based Machine Learning: A Defense against DDoS and Packet Suppression Attacks," *The Eurasia Proceedings of Science, Technology, Engineering & Mathematics*, 23, pp. 262–268. Available at: https://doi.org/10.55549/epstem.1368266.

[5] Akhiruddin, D.R. and Sutabri, T. (2023) "ANALISIS PENINGKATAN KEAMANAN PADA SIMPLE NETWORK TIME PROTOCOL (SNTP) UNTUK MENDETEKSI CYBERCRIME DALAM AKTIFITAS JARINGAN MENGGUNAKAN METODE FIREWALL," *Blantika*, 2(1), pp. 21–32. Available at: https://doi.org/10.57096/blantika.v2i1.9.

[6] Akhtar, M. and Feng, T. (2021) "An overview of the applications of Artificial Intelligence in Cybersecurity," *EAI Endorsed Transactions on Creative Technologies*, 8(29), p. 172218. Available at: https://doi.org/10.4108/eai.23-11-2021.172218.

[7] Akhtar, N., Aziz, O. and Hussain, T. (2021) "Latest trends in the Cybersecurity after the solar wind hacking attack," *Foundation University Journal of Engineering and Applied Sciences*, 1(2), pp. 14–24. Available at: https://doi.org/10.33897/fujeas.v1i2.347.

[8] Alalwan, J.A.A. (2022) "Roles and Challenges of AI-Based Cybersecurity: A Case Study," *˜ Al-œ Mağallaẗ Al-urdunniyyaẗ Fī Idāraẗ Al-a'māl*, 18(3). Available at: https://doi.org/10.35516/jjba.v18i3.196.

[9] Aleksy, M. and Korthaus, A. (1999) "Interoperability of Java-based applications and SAP's business framework state of the art and desirable developments." Available at: https://doi.org/10.1109/doa.1999.794024.

[10] Al-Fawa'reh, M., Abu-Khalaf, J., Szewczyk, P. and Kang, J.J. (2024) "MalBoT-DRL: Malware Botnet Detection Using Deep Reinforcement Learning in IoT Networks," *IEEE Internet of Things Journal*, p. 1. Available at: https://doi.org/10.1109/jiot.2023.3324053.

[11] Alghamdi, M.I. (2020) "Reviewing the effectiveness of artificial intelligence techniques against cyber security risks," *Periodicals of Engineering and Natural Sciences*, 8(4), pp. 2089–2095. Available at: https://doi.org/10.21533/pen.v8i4.1684.

[12] Alharbi, A., Seh, A.H., Alosaimi, W., Alyami, H., Agrawal, A., Kumar, R. and Khan, R.A. (2021) "Analyzing the Impact of Cyber

Security Related Attributes for Intrusion Detection Systems," *Sustainability*, 13(22), p. 12337. Available at: https://doi.org/10.3390/su132212337.

[13] Alonso, F., Samaniego, B., Farias, G. and Dormido-Canto, S. (2024) "Analysis of Cryptographic Algorithms to Improve Cybersecurity in the Industrial Electrical Sector," *Applied Sciences*, 14(7), p. 2964. Available at: https://doi.org/10.3390/app14072964.

[14] Alsunbul, S., Le, P., Tan, J. and Srinivasan, B. (2016) "A network defense system for detecting and preventing potential hacking attempts." Available at: https://doi.org/10.1109/icoin.2016.7427157.

[15] Amalberti, R., Staines, A. and Vincent, C. (2022) "Embracing multiple aims in healthcare improvement and innovation," *International Journal for Quality in Health Care*, 34(1). Available at: https://doi.org/10.1093/intqhc/mzac006.

[16] Amoresano, K. and Yankson, B. (2023) "Human Error - A Critical Contributing Factor to the Rise in Data Breaches: A Case Study of Higher Education," *Holistica*, 14(1), pp. 110–132. Available at: https://doi.org/10.2478/hjbpa-2023-0007.

[17] Andisty, M.P. and Harmain, H. (2022) "Penerapan System Application and Product (SAP) pada Administrasi Kepegawaian (Penerima Santunan Hari Tua (SHT)) di PT. Perkebunan Nusantara II Kebun Bandar Klippa," *Al-Kharaj*, 5(3), pp. 1291–1298. Available at: https://doi.org/10.47467/alkharaj.v5i3.1625.

[18] Anshari, S.F. and Retno, S. (2023) "Penerapan Metode Nine-Step Kimball Dalam Pengolahan Data History Menggunakan Data Warehouse dan Business Intelligence," *Jurnal Ilmu Komputer*, 16(1), p. 69. Available at: https://doi.org/10.24843/jik.2023.v16.i01.p07.

[19] Azevedo, N., Aquino, G., Nascimento, L., Camelo, L., Figueira, T., Oliveira, J., Figueiredo, I., Printes, A., Torné, I. and Figueiredo, C. (2023) "A Novel Methodology for Developing Troubleshooting Chatbots Applied to ATM Technical Maintenance Support," *Applied Sciences*, 13(11), p. 6777. Available at: https://doi.org/10.3390/app13116777.

[20] Baugher, J. and Qu, Y. (2024) "Create the Taxonomy for Unintentional Insider Threat via Text Mining and Hierarchical Clustering Analysis," *European Journal of Electrical Engineering and Computer Science*, 8(2), pp. 36–49. Available at: https://doi.org/10.24018/ejece.2024.8.2.608.

[21] Berger, H. and Jones, A. (2016) "Cyber Security & Ethical Hacking For SMEs." Available at: https://doi.org/10.1145/2925995.2926016.

[22] Bhakare, N.R.V., Bhakare, N.S.V., Kukade, N.M.S. and Ingole, N.D.D. (2023) "Cybersecurity in Power Systems Challenges, Strategies, and Results," *International Journal of Advanced Research in Science, Communication and Technology*, pp. 47–49. Available at: https://doi.org/10.48175/ijarsct-12910.

[23] Bitmanov, D. and Uruzbaeva, N. (2021) "РАЗРАБОТКА МЕХАНИЗМОВ КИБЕРБЕЗОПАСНОСТИ НА ФАРМАЦЕВТИЧЕСКИХ КОМПАНИЯХ КАЗАХСТАНА И ВЫГОДЫ ОТ ИХ ВНЕДРЕНИЯ (НА ПРИМЕРЕ ТОО «СК-ФАРМАЦИЯ»)," *H. Dosmuhamedov Atyndağy Atyrau Memlekettìk Universitetìnìņ Habaršysy/H. Dosmuhamedov Atyndağy Atyrau Universitetìnìņ Habaršysy* [Preprint]. Available at: https://doi.org/10.47649/vau.2021.v60.i1.06.

[24] Bojanova, I. and Galhardo, C.E.C. (2023) "Bug, Fault, Error, or Weakness: Demystifying Software Security Vulnerabilities," *IT Professional*, 25(1), pp. 7–12. Available at: https://doi.org/10.1109/mitp.2023.3238631.

[25] Bopalia, V.S. (2023) "Iterative Integrated Planning and Scheduling Model in Project Management." Available at: https://doi.org/10.2118/213382-ms.

[26] Chadha, R., Shalom, G.S., Anand, V.K. and Goel, A. (2022) "A Study on Exploit Development." Available at: https://doi.org/10.1109/icccs55188.2022.10079387.

[27] Chan, P., Barnett, T., Badawy, A.-H. and Jungwirth, P.W. (2018) "Cyber defense

through hardware security." Available at: https://doi.org/10.1117/12.2302805.

[28] Chandra, R.N. and Yulistia, Y. (2023) "Customer Relationship Management (CRM) Menggunakan Metode Pengembangan RUP pada PT XYZ," *Proceeding Multi Data Palembang Student Conference*, 2(1), pp. 463–469. Available at: https://doi.org/10.35957/mdp-sc.v2i1.4519.

[29] Chang, M., Kuhn, R. and Weil, T. (2018) "Cyberthreats and Security," *IT Professional*, 20(3), pp. 20–22. Available at: https://doi.org/10.1109/mitp.2018.032501744.

[30] Chari, G., Sheffer, B., Branavan, S.R.K. and D'ippolito, N. (2023) "Scaling Web API Integrations." Available at: https://doi.org/10.1109/icse-seip58684.2023.00007.

[31] Chary, G.V.K., Mahantesh, M., Reddy, M.N., Rohith, M. and Shanthala, P.T. (2023) "Evaluating the Effectiveness of Tree-based Machine Learning Classifiers for Cybersecurity Threat Detection." Available at: https://doi.org/10.1109/inc457730.2023.10262889.

[32] Chatterjee, A. and Prinz, A. (2022) "Applying Spring Security Framework with KeyCloak-Based OAuth2 to Protect Microservice Architecture APIs: A Case Study," *Sensors*, 22(5), p. 1703. Available at: https://doi.org/10.3390/s22051703.

[33] Chauhan, R. (2023) "Impact of Customer Relationship Management," *International Journal for Research in Applied Science and Engineering Technology*, 11(4), pp. 3059–3060. Available at: https://doi.org/10.22214/ijraset.2023.50856.

[34] Cheng, E.C.K. and Wang, T. (2022) "Institutional Strategies for Cybersecurity in Higher Education Institutions," *Information*, 13, p. 192. Available at: https://doi.org/10.3390/info13040192.

[35] Chinthamu, N. and Karukuri, M. (2023) "Data Science and Applications," *Journal of Data Science and Intelligent Systems*, 1(2). Available at: https://doi.org/10.47852/bonviewjdsis3202837.

[36] Chopra, S., Marwaha, H. and Sharma, A. (2022) "Cyber-Attacks Identification and Measures for Prevention." Available at: https://doi.org/10.19107/cybercon.2022.11.

[37] Christiandava, A.R., Azzahra, A., Nurdiana, A. and Setiabudi, B. (2023) "Re-Design Struktur Gedung Head Office Awann Group Berdasarkan Integrasi BIM Autodesk melalui Revit, Naviswork, dan SAP2000," *Jurnal Sipil Dan Arsitektur*, 1(1), pp. 16–32. Available at: https://doi.org/10.14710/pilras.1.1.2023.16-32.

[38] Corona, I.V.M., Manzano, G.A.S., Aguilar, F.A.B. and Gonzalez, Y.F.S. (2023) "Seguridad en Sistemas de Autenticación: Análisis de Vulnerabilidades y Estrategias de Mitigación," *Xikua Boletín Científico De La Escuela Superior De Tlahuelilpan*, 11(22), pp. 39–43. Available at: https://doi.org/10.29057/xikua.v11i22.10802.

[39] Damm, M., Summa, A., Nazeri, A., Dietzel, M., Frenzel, S. and Heich, W. (2022) "Employing Messenger Communication with Asset Administration Shells," *2022 IEEE 27th International Conference on Emerging Technologies and Factory Automation (ETFA)* [Preprint]. Available at: https://doi.org/10.1109/etfa52439.2022.9921283.

[40] Dangi, A.K., Pant, K., Alanya-Beltran, J., Chakraborty, N., Akram, S.V. and Balakrishna, K. (2023) "A Review of use of Artificial Intelligence on Cyber Security and the Fifth-Generation Cyber-attacks and its analysis." Available at: https://doi.org/10.1109/aisc56616.2023.10085175.

[41] Domagała, A., Grobler-Dębska, K., Wąs, J. and Kucharska, E. (2021) "Post-Implementation ERP Software Development: Upgrade or Reimplementation," *Applied Sciences*, 11(11), p. 4937. Available at: https://doi.org/10.3390/app11114937.

[42] Donepudi, P.K. (2015) *Crossing Point of Artificial Intelligence in Cybersecurity*, *American Journal of Trade and Policy*, pp. 121–128.

[43] Efuntade, O.O. and Efuntade, A.O. (2023) "Application Programming Interface (API) And Management of Web-Based Accounting

Information System (AIS): Security of Transaction Processing System, General Ledger and Financial Reporting System," *Journal of Accounting and Financial Management*, 9(6), pp. 1–18. Available at: https://doi.org/10.56201/jafm.v9.no6.2023.pg1.18.

[44] Elbes, M., Hendawi, S., AlZu'bi, S., Kanan, T. and Mughaid, A. (2023) "Unleashing the Full Potential of Artificial Intelligence and Machine Learning in Cybersecurity Vulnerability Management." Available at: https://doi.org/10.1109/icit58056.2023.10225910.

[45] Elkhannoubi, H. and Belaissaoui, M. (2015) "A framework for an effective cybersecurity strategy implementation: Fundamental pillars identification." Available at: https://doi.org/10.1109/isda.2015.7489156.

[46] Fakiha, B. (2022) "Effectiveness of Forensic Firewall in Protection of Devices from Cyberattacks," *International Journal of Safety and Security Engineering*, 12(1), pp. 77–82. Available at: https://doi.org/10.18280/ijsse.120110.

[47] Falco, G. and Rosenbach, E. (2022) "Who Is Responsible for Cybersecurity?," in *Oxford University Press eBooks*, pp. 79–103. Available at: https://doi.org/10.1093/oso/9780197526545.003.0005.

[48] Fan, L., Peng, T., Tian, R., Liu, Z., Ni, Y. and Liu, L. (2022) "RBAC Model-Based User Authority Distribution Method of Power Marketing System," *2022 4th International Conference on Power and Energy Technology (ICPET)* [Preprint]. Available at: https://doi.org/10.1109/icpet55165.2022.9918526.

[49] Farhi, N., Koenigstein, N. and Shavitt, Y. (2023) "Detecting Security Patches via Behavioral Data in Code Repositories," *arXiv (Cornell University)* [Preprint]. Available at: https://doi.org/10.48550/arxiv.2302.02112.

[50] Fauzi, E., Yuliani, S., Syukriyah, Y. and Zakiah, A. (2023) "Model of NFT Implementation on Web SSO over OpenID Connect and Oauth 2.0 protocols," *Intecoms*, 6(2), pp. 605–616. Available at: https://doi.org/10.31539/intecoms.v6i2.6972.

[51] Fayayola, N.O.A., Olorunfemi, N.O.L. and Shoetan, N.P.O. (2024) "DATA PRIVACY AND SECURITY IN IT: A REVIEW OF TECHNIQUES AND CHALLENGES," *Computer Science & IT Research Journal*, 5(3), pp. 606–615. Available at: https://doi.org/10.51594/csitrj.v5i3.909.

[52] Firdaus, M.A.R., Asalina, R.U., Nurdiana, A. and Setiabudi, B. (2023) "Model 5D Gedung Dekanat dan Perkuliahan Fakultas Kesehatan Masyarakat, Universitas Diponegoro," *Jurnal Sipil Dan Arsitektur*, 1(3), pp. 45–59. Available at: https://doi.org/10.14710/pilars.1.3.2023.45-59.

[53] Galinec, D. and Steingartner, W. (2017) "Combining cybersecurity and cyber defense to achieve cyber resilience." Available at: https://doi.org/10.1109/informatics.2017.8327227.

[54] Ghazal, T.M., Hasan, M.K., Zitar, R.A., Al-Dmour, N.A., Al-Sit, W.T. and Islam, S. (2022) "Cybers Security Analysis and Measurement Tools Using Machine Learning Approach." Available at: https://doi.org/10.1109/icaic53980.2022.9897045.

[55] Ghernouti-Hélie, S. (2010) "A National Strategy for an Effective Cybersecurity Approach and Culture." Available at: https://doi.org/10.1109/ares.2010.119.

[56] Gichuru, C.K. and Onjure, C.O. (2019) "Influence of Stakeholders' Engagement Practices on Performance of System Applications Products for Oil and Gas Upgrade Project at Kenya Pipeline Company Nakuru Depot," *International Journal of Business & Management*, 7(10). Available at: https://doi.org/10.24940/theijbm/2019/v7/i10/bm1910-009.

[57] González-Muñoz, J., Casado, M., Garabato, D., Nóvoa, F.J. and Dafonte, C. (2023) "Hardening of a Continuous Behavior-based Authentication Distributed System." Available at: https://doi.org/10.17979/spudc.000024.31.

[58] Guo, C., Lang, F., Wang, Q. and Lin, J. (2022) "UP-SSO: Enhancing the User Privacy of SSO by Integrating PPID and SGX." Available at:

https://doi.org/10.1109/ieeeconf52377.2022.10013340.

[59] Hanafi, R., Munir, N., Suwatno, N. and Furqon, C. (2023) "Implementation of Enterprise Architecture with Leadership Moderation Effects as a Performance Model for Regency/City Local Government Agencies in West Java Province," *Journal of Law and Sustainable Development*, 11(9), p. e548. Available at: https://doi.org/10.55908/sdgs.v11i9.548.

[60] Haripriya, M.P., Jolly, A. and Venkadesh, P. (2023) "Cyber Security Unveiled: Trends and Protections in the Digital World," *Indian Scientific Journal of Research in Engineering and Management*, 07(07). Available at: https://doi.org/10.55041/ijsrem24720.

[61] Haryadi, E., Wijayanti, D. and Widyastuti, I. (2022) *Perancangan ERP S4Hana Cloud Pada Modul Material Management Menggunakan Metode SAP Active*, *BINA INSANI ICT JOURNAL*, pp. 11–21.

[62] Hasan, Md.M., Islam, M.U. and Uddin, J. (2023) "Advanced Persistent Threat Identification with Boosting and Explainable AI," *SN Computer Science/SN Computer Science*, 4(3). Available at: https://doi.org/10.1007/s42979-023-01744-x.

[63] Hisbullah, M.D., Sari, C.A., Rachmawanto, E.H., Handoko, L.B., Umam, C. and Isinkaye, F. (2023) "Hybrid Encryption Based on Fernet and Rivest Shamir Adleman (RSA)." Available at: https://doi.org/10.1109/isemantic59612.2023.10295309.

[64] Holubiev, V., Simashko, V., Jarmoch, E., Majda, P., Taraj, M. and Bursova, J. (2022) "Toward Building Specialized Information Systems as Software Platforms," *2022 12th International Conference on Advanced Computer Information Technologies (ACIT)* [Preprint]. Available at: https://doi.org/10.1109/acit54803.2022.9913128.

[65] Horowitz, B., Beling, P., Skadron, K., Williams, R.D. and Melvin, W. (2015) *Security Engineering Project*. Available at: https://doi.org/10.21236/ada626823.

[66] Hummelholm, A. (2023) "AI-based quantum-safe cybersecurity automation and orchestration for edge intelligence in future networks," *Proceedings of the ... European Conference on Information Warfare and Security*, 22(1), pp. 696–702. Available at: https://doi.org/10.34190/eccws.22.1.1211.

[67] Hussain, S., Iqbal, A., Hussain, S.M.S., Zanero, S., Shikfa, A., Ragaini, E., Khan, I. and Alammari, R. (2023) "A novel hybrid methodology to secure GOOSE messages against cyberattacks in smart grids," *Scientific Reports*, 13(1). Available at: https://doi.org/10.1038/s41598-022-27157-z.

[68] Jain, N. and Cherukuri, A.K. (2023) "Revisiting Fully Homomorphic Encryption Schemes," *arXiv (Cornell University)* [Preprint]. Available at: https://doi.org/10.48550/arxiv.2305.05904.

[69] Jarwal, A., Kumar, K. and Kumar, A. (2023) "Secure Data Encryption Scheme for Cloud Computing," *International Journal for Research in Applied Science and Engineering Technology*, 11(5), pp. 897–902. Available at: https://doi.org/10.22214/ijraset.2023.51058.

[70] Jerbi, D. (2023) "Beyond Firewalls: Navigating the Jungle of Emerging Cybersecurity Trends," *Journal of Current Trends in Computer Science Research*, 2(2), pp. 191–195.

[71] Jinhong, F. (2024) "Cross-Platform and Multi-Terminal Collaborative Software Information Security Strategy." Available at: https://doi.org/10.1109/icmcsi61536.2024.00121.

[72] Jony, A.I. and Hamim, S.A. (2024) "Navigating the Cyber Threat Landscape: A Comprehensive Analysis of Attacks and Security in the Digital Age," *Journal of Information Technology and Cyber Security*, 1(2), pp. 53–67. Available at: https://doi.org/10.30996/jitcs.9715.

[73] Kalouptsoglou, I., Siavvas, M., Kehagias, D., Chatzigeorgiou, A. and Ampatzoglou, A. (2022) "Examining the Capacity of Text Mining and Software Metrics in Vulnerability Prediction," *Entropy*, 24(5), p. 651. Available at: https://doi.org/10.3390/e24050651.

[74] Kante, M., Sharma, V. and Gupta, K. (2024) "Mitigating ransomware attacks through cyber threat intelligence and machine learning," *Indonesian Journal of Electrical Engineering and Computer Science*, 33(3), p. 1958. Available at: https://doi.org/10.11591/ijeecs.v33.i3.pp1958-1965.

[75] Kedarya, T. and Elalouf, A. (2023) "Risk Management Strategies for the Banking Sector to Cope with the Emerging Challenges," *Foresight and STI Governance/Forsajt*, 17(3), pp. 68–76. Available at: https://doi.org/10.17323/2500-2597.2023.3.68.76.

[76] Kemper, A., Kossmann, D. and Matthes, F. (1998) "SAP R/3 (tutorial): a database application system," *SIGMOD '98: Proceedings of the 1998 ACM SIGMOD International Conference on Management of Data* [Preprint]. Available at: https://doi.org/10.1145/276304.276351.

[77] Ketoma, V.K., Vanderdonckt, J. and Meixner, G. (2023) "Towards Flexible Authoring and Personalization of Virtual Reality Applications for Training," *Proceedings of the ACM on Human-computer Interaction*, 7(EICS), pp. 1–37. Available at: https://doi.org/10.1145/3593241.

[78] Khalid, N.E.T., Aldarwish, N.A.J.Y. and AYassin, N.A. (2023) "Challenges in AutoML and Declarative Studies Using Systematic Literature Review," *Applied Data Science and Analysis*, 2023, pp. 118–125. Available at: https://doi.org/10.58496/adsa/2023/011.

[79] Khaliq, K., Rahim, N.Z.A., Hamid, K., Ibrar, M., Ahmad, U. and Ullah, M.U. (2024) "Ransomware Attacks: Tools and Techniques for Detection." Available at: https://doi.org/10.1109/iccr61006.2024.10532926.

[80] Kumar, S. (2023) "SAP HANA Data Volume Management," *arXiv (Cornell University)* [Preprint]. Available at: https://doi.org/10.48550/arxiv.2305.17723.

[81] KumarGoutam, R. (2015) "Importance of Cyber Security," *International Journal of Computer Applications*, 111(7), pp. 14–17. Available at: https://doi.org/10.5120/19550-1250.

[82] Laher, R.R., Masci, F.J., Rebull, L.M., Schurr, S.D., Burt, W., Laity, A., Swain, M., Shupe, D.L., Groom, S., Rusholme, B., Kong, M.-S., Good, J.C., Gorjian, V., Akeson, R., Fulton, B.J., Ciardi, D.R. and Carey, S. (2023) "Upgraded Thoth: Software for Data Visualization and Statistics," *Analytics*, 2(1), pp. 284–295. Available at: https://doi.org/10.3390/analytics2010015.

[83] Larriva-Novo, X., Sánchez-Zas, C., Villagrá, V.A., Marín-Lopez, A. and Berrocal, J. (2023) "Leveraging Explainable Artificial Intelligence in Real-Time Cyberattack Identification: Intrusion Detection System Approach," *Applied Sciences*, 13(15), p. 8587. Available at: https://doi.org/10.3390/app13158587.

[84] Li, J., Lin, Z. and Zhang, X. (2023) "The Study on the Effectiveness of Sustainable Customer Relationship Management: Evidence from the Online Shopping Industry," *Sustainability*, 15(7), p. 5911. Available at: https://doi.org/10.3390/su15075911.

[85] Li, L., Thakur, K. and Ali, M.L. (2020) "Potential Development on Cyberattack and Prospect Analysis for Cybersecurity," *2020 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)* [Preprint]. Available at: https://doi.org/10.1109/iemtronics51293.2020.9216374.

[86] Lie, I. and Ernestine, J. (2016) "Construction Project Accounting System based on the Earned Value Management and Management Accounting Framework in Road and Bridge Project." Available at: https://doi.org/10.15224/978-1-63248-110-8-38.

[87] Lim, J., Lau, Y.L., Chan, L.K.M., Goo, J.M.T.P., Zhang, H., Zhang, Z. and Guo, H. (2023) "CVE Records of Known Exploited Vulnerabilities." Available at: https://doi.org/10.1109/icccs57501.2023.10150856.

[88] Lin, P.-C., Shu, M.-H., Hsu, B.-M., Hu, C.-M. and Huang, J.-C. (2022) "Supply Chain Management System for Automobile Manufacturing Enterprises Based on SAP,"

Wireless Communications and Mobile Computing, 2022, pp. 1–10. Available at: https://doi.org/10.1155/2022/5901633.

[89] Liu, M., Peng, X., Marcus, A., Treude, C., Xie, J., Xu, H. and Yang, Y. (2022) "How to formulate specific how-to questions in software development?," *Proceedings of the 30th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering* [Preprint]. Available at: https://doi.org/10.1145/3540250.3549160.

[90] Liu, P., Zhao, Y., Cai, H., Fazzini, M., Grundy, J. and Li, L. (2022) "Automatically detecting API-induced compatibility issues in Android apps: a comparative analysis (replicability study)." Available at: https://doi.org/10.1145/3533767.3534407.

[91] Lourens, M., Dabral, A.P., Gangodkar, D., Rathour, N., Tida, C.N. and Chadha, A. (2022) "Integration of AI with the Cybersecurity: A detailed Systematic review with the practical issues and challenges." Available at: https://doi.org/10.1109/ic3i56241.2022.10073040.

[92] Maidine, K. and El-Yahyaoui, A. (2023) "Cloud Identity Management Mechanisms and Issues." Available at: https://doi.org/10.1109/cloudtech58737.2023.10366178.

[93] Majerník, M., Daneshjo, N., Malega, P., Drábik, P., Ševčíková, R. and Vravec, J. (2023) "Integrated Management of the Environment-Safety Risks in the Thermal Power Station," *Polish Journal of Environmental Studies*, 32(5), pp. 4725–4738. Available at: https://doi.org/10.15244/pjoes/168290.

[94] Mangaoang, N.E.F. (2024) "Common Vulnerabilities and Exposures Assessment of Private Higher Educational Institutions Using Web Application Security," *Deleted Journal*, 20(5s), pp. 668–676. Available at: https://doi.org/10.52783/jes.2288.

[95] Martinez, Z.H., Moreno, P.M., Camacho, J.A.V. and Vega, G.C. (2023) "Study on the Use of Defect Metrics in the Software Development Process. Flaws and Vulnerabilities." Available at: https://doi.org/10.1109/icev59168.2023.10329656.

[96] Mathieu, R.G. and Turovlin, A.E. (2023) "Lost in the middle – a pragmatic approach for ERP managers to prioritize known vulnerabilities by applying classification and regression trees (CART)," *Information & Computer Security/Information and Computer Security*, 31(5), pp. 655–674. Available at: https://doi.org/10.1108/ics-02-2023-0027.

[97] Möller, D.P.F. and Vakilzadian, H. (2023) "Cybersecurity Risk in Digitalization of Infrastructure Systems: A Use Case." Available at: https://doi.org/10.1109/eit57321.2023.10187348.

[98] Momani, A., Al-Hawari, T. and Tahat, S. (2023) "A Framework to Diagnose the Business and Evaluate Upgrade Plans in SMEs," *Management and Production Engineering Review* [Preprint]. Available at: https://doi.org/10.24425/mper.2021.138528.

[99] More, N.S., Kotasthane, N.V., Ahire, N.M. and Shelke, N.S. (2024) "Virtual Assistance for Banking System using AI and ML," *International Journal of Advanced Research in Science, Communication and Technology*, pp. 641–645. Available at: https://doi.org/10.48175/ijarsct-18366.

[100] Muhaimin, M. (2022) "PERAN APARAT PENGAWASAN INTERN PEMERINTAH DALAM MENGIMPLEMENTASIKAN MANAJEMEN RISIKO PEMERINTAH DAERAH," *Kajen*, 6(01), pp. 54–71. Available at: https://doi.org/10.54687/jurnalkajenv6i01.6.

[101] Munjala, M.B. (2024) "Exploring Analytics in SAP S/4HANA Cloud: Capabilities, Integration, and Business Value," *Indian Scientific Journal of Research in Engineering and Management*, 08(01), pp. 1–13. Available at: https://doi.org/10.55041/ijsrem27868.

[102] Murthy, J.S. and Shilpa, H.L. (2021) "Network Software Vulnerability Identifier using J48 decision tree algorithm," *International Journal for Research in Applied Science and Engineering Technology*, 9(8), pp. 1889–1892. Available at: https://doi.org/10.22214/ijraset.2021.37685.

[103] Myronenko, O. (2023) "Assessing the efficiency of application of project management in the field of engineering of innovative developments," *Eastern-European Journal of Enterprise Technologies*, 4(13 (124)), pp. 94–100. Available at: https://doi.org/10.15587/1729-4061.2023.285542.

[104] Neetha, S.S., Bhuvana, J. and Suchithra, R. (2023) "An Efficient Image Encryption Reversible Data Hiding Technique to Improve Payload and High Security in Cloud Platforms." Available at: https://doi.org/10.1109/iscon57294.2023.10112201.

[105] Nwobodo, N.L.K., Nwaimo, N.C.S. and Adegbola, N.A.E. (2024) "Enhancing cybersecurity protocols in the era of big data and advanced analytics," *GSC Advanced Research and Reviews*, 19(3), pp. 203–214. Available at: https://doi.org/10.30574/gscarr.2024.19.3.0211.

[106] Oladokun, B., Oloniruha, E., Mazah, D. and Okechukwu, O. (2024) "Cybersecurity risks in libraries: Why universities libraries in African need to promote cyberethical practices," *Southern African Journal of Security* [Preprint]. Available at: https://doi.org/10.25159/3005-4222/15320.

[107] Pal, N.Prof.R., Shaikh, N.M., Sagvekar, N.J. and Tiwari, N.P. (2024) "Data Resilience: Secure Emergency Backup on Cloud," *International Journal of Advanced Research in Science, Communication and Technology*, pp. 29–35. Available at: https://doi.org/10.48175/ijarsct-17805.

[108] Pan, J., Chang, C.-C., Xie, Z. and Chen, Y. (2023) "EDALearn: A Comprehensive RTL-to-Signoff EDA Benchmark for Democratized and Reproducible ML for EDA Research," *arXiv (Cornell University)* [Preprint]. Available at: https://doi.org/10.48550/arxiv.2312.01674.

[109] Papaspirou, V., Papathanasaki, M., Maglaras, L., Kantzavelou, I., Douligeris, C., Ferrag, M.A. and Janicke, H. (2023) "A Novel Authentication Method That Combines Honeytokens and Google Authenticator," *Information*, 14(7), p. 386. Available at: https://doi.org/10.3390/info14070386.

[110] Patel, D., Patel, H., Sultana, K.Z. and Anu, V. (2023) "Programmer Cognition Failures as the Root Cause of Software Vulnerabilities: A Preliminary Review." Available at: https://doi.org/10.1109/ietc57902.2023.10152150.

[111] Patel, Y., Rughani, P.H. and Desai, D. (2022) "Analyzing Security Vulnerability and Forensic Investigation of ROS2: A Case Study." Available at: https://doi.org/10.1145/3573910.3573912.

[112] Phatangare, S. (2024) "Multi-Level Encryption System using AES and RSA Algorithms," *International Journal for Research in Applied Science and Engineering Technology*, 12(5), pp. 4043–4051. Available at: https://doi.org/10.22214/ijraset.2024.62420.

[113] Poroca, F.B. (2023) "O sistema SAP S/4HANA e a transformação digital nas organizações," *Núcleo Do Conhecimento*, pp. 54–77. Available at: https://doi.org/10.32749/nucleodoconhecimento.com.br/tecnologia/transformacao-digital.

[114] Prajwal, M. and G, Deepak. (2023) "Investigating Perceived Security and Usability of Secure Shield: An Advanced Multi-Factor Authentication System - A Survey," *Deleted Journal*, pp. 1–5. Available at: https://doi.org/10.48001/jowacs.2023.111-5.

[115] Puthal, D., Mohanty, S.P., Nanda, P. and Choppali, U. (2017) "Building Security Perimeters to Protect Network Systems Against Cyber Threats [Future Directions]," *IEEE Consumer Electronics Magazine*, 6(4), pp. 24–27. Available at: https://doi.org/10.1109/mce.2017.2714744.

[116] Qammar, A., Wang, H., Ding, J., Naouri, A., Daneshmand, M. and Ning, H. (2023) "Chatbots to ChatGPT in a Cybersecurity Space: Evolution, Vulnerabilities, Attacks, Challenges, and Future Recommendations," *arXiv (Cornell University)* [Preprint]. Available at: https://doi.org/10.48550/arxiv.2306.09255.

[117] Qian, X. (2023) "Network security and computer program," *Applied and*

Computational Engineering, 5(1), pp. 744–749. Available at: https://doi.org/10.54254/2755-2721/5/20230688.

[118] Raazi, N.I.M., Dwitawati, N.I. and Nabila, N.P. (2023) "Uji Vulnerability Assessment Dalam Mengetahui Tingkat Keamanan Web Aplikasi Sistem Informasi Laporan Diskominfo Dan Sandi Aceh," *Journal of Information Technology*, 4(1), pp. 1–15. Available at: https://doi.org/10.22373/jintech.v4i1.2409.

[119] Raj, P. (2024) "Continuous Integration for New Service Deployment and Service Validation Script for Vault," *Indian Scientific Journal of Research in Engineering and Management*, 08(06), pp. 1–5. Available at: https://doi.org/10.55041/ijsrem35565.

[120] Rama, P. and Keevy, M. (2023) "Public cybersecurity awareness good practices on government-led websites," *International Journal of Research in Business and Social Science*, 12(7), pp. 94–104. Available at: https://doi.org/10.20525/ijrbs.v12i7.2840.

[121] Ramli, H. and Alifsyah, M.Y. (2023) "Analisis Keamanan Komputer Terhadap Serangan Distributed Denial of Service (DDOS)," *Journal of Renewable Energy and Smart Device*, 1(1), pp. 25–30. Available at: https://doi.org/10.61220/joresd.v1i1.235.

[122] Riyadi, A.A., Amsury, F., Saputra, I., Pattiasina, T. and Jupriyanto, J. (2022) "COMPARATIVE ANALYSIS OF THE K-NEAREST NEIGHBOR ALGORITHM ON VARIOUS INTRUSION DETECTION DATASETS," *Jurnal Riset Informatika*, 4(1), pp. 127–132. Available at: https://doi.org/10.34288/jri.v4i1.341.

[123] Sadat, S.E., Lodin, H. and Ahmadzai, N. (2023) "Highly Secure and Easy to Remember Password-Based Authentication Approach," *Journal for Research in Applied Sciences and Biotechnology*, 2(1), pp. 134–141. Available at: https://doi.org/10.55544/jrasb.2.1.18.

[124] Sahu, C.K., Dash, S.S., Sinha, A., Baghel, R., Sahu, R.K. and Ratha, A.K. (2024) "User-Centric Approach to Fortify Cloud Data Security with Hybrid Cryptosystem Methods." Available at: https://doi.org/10.1109/icaect60202.2024.10468782.

[125] Sangewar, S. and Gugulothu, S. (2023) "Securing Images using Encryption & Decryption." Available at: https://doi.org/10.1109/icces57224.2023.10192684.

[126] Sasikala, D. and Sharma, K.V. (2022) "Deployment of Artificial Intelligence with Bootstrapped Meta-Learning in Cyber Security," *Journal of Trends in Computer Science and Smart Technology*, 4(3), pp. 139–152. Available at: https://doi.org/10.36548/jtcsst.2022.3.003.

[127] Seneviratne, S.M.C. and Colombage, L. (2023) "The impact of User-Characteristics and Organizational-Characteristics on End-user Satisfaction with Enterprise Resource Planning (ERP) systems," *International Journal of Financial, Accounting, and Management*, 5(1), pp. 75–95. Available at: https://doi.org/10.35912/ijfam.v5i1.1295.

[128] Sharma, A., Upadhyay, D. and Sharma, S. (2024) "Enhancing Blockchain Security: A Novel Approach to Integrated Malware Defense Mechanisms," *Engineering Research Express* [Preprint]. Available at: https://doi.org/10.1088/2631-8695/ad4ba7.

[129] Sharma, C. and Maurya, S. (2020) "A REVIEW: IMPORTANCE OF CYBER SECURITY AND ITS CHALLENGES TO VARIOUS DOMAINS," *International Journal of Technical Research & Science*, Special(Issue3), pp. 46–54. Available at: https://doi.org/10.30780/specialissue-icaccg2020/015.

[130] Shekaili, M., Balushi, I., Kumar, N. and Marin, E. (2023) "Improved Operational Excellence in Oil and Gas Production Management Through New Well Management System." Available at: https://doi.org/10.2118/216073-ms.

[131] Shen, K., Zhang, Y., Bao, L., Wan, Z., Li, Z. and Wu, M. (2023) "Patchmatch: A Tool for Locating Patches of Open Source Project Vulnerabilities." Available at: https://doi.org/10.1109/icse-companion58688.2023.00049.

[132] Shmeleva, A.N. (2020) "Telecommunication Networks Security as a Part of Cybersecurity."

Available at: https://doi.org/10.1109/itqmis51053.2020.9322907.

[133] Shrivastava, P. and Yadav, R.K. (2023) "Cyber-Attacks Detection Using Intelligent Intrusion System (IDS) Along With Deep Learning: Novel Approach." Available at: https://doi.org/10.1109/icccnt56998.2023.10306742.

[134] Shterev, Y. (2022) "Concepts of Cyber Security," *Inovativno STEM Obrazovanie*, 4(1), pp. 79–88. Available at: https://doi.org/10.55630/stem.2022.0411.

[135] Sipos, Z. (2023) "Cybersecurity in Algeria," *Journal of Security and Sustainability Issues*, 13(1), pp. 65–73. Available at: https://doi.org/10.47459/jssi.2023.13.6.

[136] Sirse, S., Khanzode, S. and Bhide, A. (2023) "ERP: SAP S/4HANA Cloud RISE Enterprise Solution Automation with Artificial Intelligence Features," *International Journal for Research in Applied Science and Engineering Technology*, 11(10), pp. 2055–2062. Available at: https://doi.org/10.22214/ijraset.2023.56384.

[137] Škanata, D. (2020) "Improving Cyber Security with Resilience," *Annals of Disaster Risk Sciences*, 3(1). Available at: https://doi.org/10.51381/adrs.v3i1.43.

[138] Škorić, M. (2021) "PLANIRANJE RESURSA PREDUZEĆA – ERP SISTEM," *Zbornik Radova Fakulteta Tehničkih Nauka/Zbornik Radova Fakulteta TehničKih Nauka*, 36(10), pp. 1775–1778. Available at: https://doi.org/10.24867/14gi18skoric.

[139] Sofjan, I.P., Salik, I. and Panzica, P.J. (2023) "SAP BusinessObjects in Medical Informatics," *Curēus* [Preprint]. Available at: https://doi.org/10.7759/cureus.40208.

[140] Sri, P.L., Krishna, Ch.N., Sai, A.D. and Roshini, Saini. (2023) "Concealing the Data using Cryptography." Available at: https://doi.org/10.1109/icais56108.2023.10073878.

[141] Supit, Y. and Irwansyah, N.E. (2024) "Kajian Keamanan Sistem Informasi Akademik Menggunakan Framework COBIT 5," *Teknomatika*, 17(1), pp. 10–24. Available at: https://doi.org/10.30989/teknomatika.v17i1.1330.

[142] Syauqie, A.S., Puspitasari, W. and Septiningrum, L. (2023) "EVALUATION OF SAP IMPLEMENTATION ACCEPTANCE WITH THEORY OF PLANNED BEHAVIOR AT PT KERETA API INDONESIA (PERSERO)," *Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika*, 8(1), pp. 66–76. Available at: https://doi.org/10.29100/jipi.v8i1.3277.

[143] Tan, X., Lv, X., Jiang, J. and Zhang, L. (2024) "Understanding Real-time Collaborative Programming: a Study of Visual Studio Live Share," *ACM Transactions on Software Engineering and Methodology* [Preprint]. Available at: https://doi.org/10.1145/3643672.

[144] Teja, K., Abhijith, K., Deepak, O.N., Hanish, T.S., Chaitanya, G.K. and Subramanyam, M.M. (2023) "Prevention of Attacks and Flow Control of Firewalls." Available at: https://doi.org/10.1109/icaccs57279.2023.10112739.

[145] Thant, K.S. and Tin, H.H.K. (2023) "LEARNING THE EFFICIENT ESTIMATION TECHNIQUES FOR SUCCESSFUL SOFTWARE PROJECT MANAGEMENT," *Innovare Journal of Engineering & Technology*, pp. 4–8. Available at: https://doi.org/10.22159/ijet.2023.v11i1.47605.

[146] Tripathy, A., Van Deventer, J., Paniagua, C. and Delsing, J. (2022) "Interoperability Between ROS and OPC UA: A Local Cloud-Based Approach." Available at: https://doi.org/10.1109/icps51978.2022.9816962.

[147] Turken, G., Naizabayeva, L., Satymbekov, M. and Abdiakhmetova, Z. (2023) "Research and Development of Enterprise Data Warehouse Based on SAP BW Modeling." Available at: https://doi.org/10.1109/sist58284.2023.10223551.

[148] Tyllis, N., Ullah, F. and Uzair, M. (2023) "An Exploratory Study of Vulnerabilities in Big Data Systems." Available at: https://doi.org/10.1109/bigdata59044.2023.10386921.

[149] Umoga, N.U.J., Sodiya, N.E.O., Amoo, N.O.O. and Atadoga, N.A. (2024) "A critical review of emerging cybersecurity threats in financial technologies," *International Journal of Science and Research Archive*, 11(1), pp. 1810–1817. Available at: https://doi.org/10.30574/ijsra.2024.11.1.0284.

[150] Vinnakota, T. (2016) "A Second Order Cybernetic Model for Governance of Cyber Security in Enterprises." Available at: https://doi.org/10.1109/iacc.2016.136.

[151] Vitale, F., McGrenere, J., Tabard, A., Beaudouin-Lafon, M. and Mackay, W.E. (2017) "High Costs and Small Benefits." Available at: https://doi.org/10.1145/3025453.3025509.

[152] Wallen, T. (2022) "The age of holistic consolidation and automation of cyber security," *Computer Fraud & Security*, 2022(4). Available at: https://doi.org/10.12968/s1361-3723(22)70571-4.

[153] Wang, M., Xie, X., Zhang, X. and Zhang, L. (2022) "Universal accelerator software and hardware collaborative design for YOLO algorithm," *International Conference on Electronic Information Technology (EIT 2022)* [Preprint]. Available at: https://doi.org/10.1117/12.2638600.

[154] Wang, T. (2022) "Troubleshooting Configuration Errors via Information Retrieval and Configuration Testing." Available at: https://doi.org/10.1109/iaecst57965.2022.10062229.

[155] Wang, Y., Ma, S., Wang, J., Jiao, X., Wang, H. and Pu, W. (2023) "Application of project management system in construction machinery enterprises," *BCP Business & Management*, 48, pp. 236–239. Available at: https://doi.org/10.54691/bcpbm.v48i.5272.

[156] Watney, M. (2024) "Exploring South Africa's Cybersecurity Legal Framework regulating Information Confidentiality, Integrity, and Availability," *Proceedings of the ... International Conference on Information Warfare and Security/˜ the œProceedings of the ... International Conference on Information Warfare and Security*, 19(1), pp. 430–437. Available at: https://doi.org/10.34190/iccws.19.1.1999.

[157] Williams, R., Gavazzi, A. and Kirda, E. (2023) "Solder: Retrofitting Legacy Code with Cross-Language Patches." Available at: https://doi.org/10.1109/saner56733.2023.00015.

[158] Xiao, Y.-A., Yang, C., Wang, B. and Xiong, Y. (2024) "Accelerating Patch Validation for Program Repair With Interception-Based Execution Scheduling," *IEEE Transactions on Software Engineering*, 50(3), pp. 618–635. Available at: https://doi.org/10.1109/tse.2024.3359969.

[159] Xu, Y., Jian, X., Li, T., Zou, S. and Li, B. (2023) "Blockchain-Based Authentication Scheme with an Adaptive Multi-Factor Authentication Strategy," *Journal of Mobile Information Systems*, 2023, pp. 1–13. Available at: https://doi.org/10.1155/2023/4764135.

[160] Xuan, H. and Manohar, M. (2023) "Intrusion Detection System with Machine Learning and Multiple Datasets," *arXiv (Cornell University)* [Preprint]. Available at: https://doi.org/10.48550/arxiv.2312.01941.

[161] Xue, Z. and Dong, B. (2023) "Research on software and hardware resource configuration of relay protection device." Available at: https://doi.org/10.1109/cieec58067.2023.10165868.

[162] Yuan, H., Wang, Z., Chen, Z., Gong, Y., Lu, J., Hu, Y., Li, L. and Qian, F. (2023) "A Fine-Grained Access Control Method Based on Role Permission Management." Available at: https://doi.org/10.1109/icdcece57866.2023.10150760.

[163] Yusif, S. and Hafeez-Baig, A. (2021) "A Conceptual Model for Cybersecurity Governance," *Journal of Applied Security Research*, 16(4), pp. 490–513. Available at: https://doi.org/10.1080/19361610.2021.1918995.

[164] Zelmati, M., Oulqaid, Z. and Elouadi, A. (2023) "Real-time Tracking of Auditing Process Progress with a Customizable Application for Cybersecurity Standards Compliance: A Case Study on ISO 27001 and TISAX." Available at:

https://doi.org/10.1109/wincom59760.2023.10322925.

[165] Zeng, H., Liu, H., Zhang, J., Sun, M. and Wang, T. (2022) “Design of Remote Upgrade System for Data Processing Unit in Marine Engine Room Simulator,” *Applied Sciences*, 12(18), p. 9107. Available at: https://doi.org/10.3390/app12189107.

[166] Zhao, F., Lu, Z., Liang, Y., Wang, Y. and He, T. (2022) “Research on Intelligent Question Answering System under Operation and Maintenance Knowledge Graph.” Available at: https://doi.org/10.1109/mlke55170.2022.00066.

[167] Zhao, Y., Li, L., Liu, K. and Grundy, J. (2022) “Towards automatically repairing compatibility issues in published Android apps,” *Proceedings of the 44th International Conference on Software Engineering* [Preprint]. Available at: https://doi.org/10.1145/3510003.3510128.