International Journal of Engineering & Scientific Research
Vol.13 Issue 02, February 2025
ISSN: 2347-6532 Impact Factor: 8.076
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Security and Reliability of Mainframes in Financial Institutions

First Author:Janakiram Thumati

Abstract

Security is paramount in financial institutions where personal and financial data processing and transactions are at risk of hacking. In order to limit unauthorized access and protect data, mainframes apply multiple security measures such as encryption, access authorization, logging, and intrusion detection. Security solutions based on mainframe capabilities can help financial institutions meet compliance requirements. Mainframes use a multilayered security system to protect confidential information and important operations in the banking sector. This study examines the security and reliability of mainframes in financial institutions. Utilizing data from IBM XForce Exchange and the Verizon Data Breach Investigations Report (DBIR), the researcher analyzed current threats, evaluated the effectiveness of mitigation strategies, and assessed the reliability of mainframe systems. The findings provide insights into best practices and areas for improvement, contributing to enhanced security and reliability in financial operations.

Keywords:

financial institutions; mainframe; cybersecurity; cybersecurity vulnerabilities; information technology.

Author correspondence:

First Author, Janakiram Thumati
Doctorate
Affiliation
Email: janiyadav@gmail.com

1. Introduction

Since its inception in the early 1900s, Information Technology (IT) has become one of the most valuable and indispensable assets to modern business [1]. Organizations need to have an efficient IT infrastructure to support business-related tasks, systems, and processes [18]. In addition to the typical desktop personal computers that most employees have at their workplace, there is much in the backend infrastructure that hosts valuable information related to the organization, employees, customers, and other stakeholders. Such crucial systems should be continuously available with minimum interruptions to serve the business, given that the majority of key applications are highly dependent on them [1]. In instances when key IT systems fail to perform as designed, the financial well-being of an organization may be at risk. For instance, a study published by CA Technologies of companies in the US and Europe projected that IT downtime results in over $26 billion a year of lost revenue [10].

An Emerson Network Power study also found that IT-related downtime costs organizations $5,600 per minute, regardless of the industry [1]. In 2013, Amazon's website was unavailable for nearly 30 minutes, and this led to a loss of at least $66,000 per minute in revenue statistics relating to the potential failure of IT systems in organizations underscore the need to guarantee the reliability and stability of IT systems such as mainframe.

Since its release in 1964 by IBM, the mainframe has been used in organizations for decades and continues to be of great importance to business processes [20]. Although there have been improvements in operating systems and other IT infrastructure, many businesses still prefer to use mainframe servers, given their history of reliability and success with those mainframes. Mainframes tend to serve large corporations that are still operating legacy applications initially developed in the 1960s and 1970s [12]. For instance, Walmart has been using mainframes since 1975 to gather data about customer transactions that are considered to help improve efficiency. Visa also uses mainframe platforms in its business structure and can process nearly 90 billion transactions annually [10].

Mainframes have been the foundation of IT infrastructure in key financial institutions for years, providing unparalleled processing power, reliability, and security. In an era where cyber threats are becoming progressively sophisticated and data breaches are regular, the security and reliability of mainframe systems are of utmost importance. Financial institutions that handle vast amounts of sensitive financial data depend on the robust architecture of mainframes to ensure the integrity and confidentiality of their operations [20]. This study aims to explore the current state of mainframe security and reliability within financial institutions, identifying key challenges and evaluating the effectiveness of existing measures. By analyzing data from various financial entities, this study sought to provide insights into the best practices and potential areas for improvement in securing these critical systems.

Across the existing literature, several studies have underscored the multifaceted nature of the security threats within mainframe computers. In particular, a recent report by IBM in 2022 indicated that while mainframes are inherently secure, they are not immune to cyberattacks. Such vulnerabilities were noted by several other studies that identified common cyberattacks in mainframes, such as inadequate configuration and outdated security protocols. Additional findings also indicate that the other group of vulnerabilities in the mainframe emanates from insider threats, malware, and external hacking attempts as significant risks to mainframe security [17].

Several researchers have emphasized the various security threats facing mainframes. According to a report by IBM (2020), mainframes, while inherently secure, are not immune to cyber-attacks, with vulnerabilities often arising from inadequate configuration and outdated security protocols (IBM, 2022). A study by Smith et al. (2021) identified insider threats, malware, and external hacking attempts as significant risks to mainframe security. The widespread use of mainframes in organizations cannot be underestimated. According to a recent report by Garnter (2022), the IBM mainframe operating systems remain to be one of the most valuable platforms for business enterprises worldwide, hosting nearly 90% of businesses' most critical missions and applications. In typical cases, businesses are less likely to adopt the same steps or procedures to mitigate configuration errors and identify them on the mainframe as they do in other operating systems. With this in mind, it is expected that high-risk vulnerabilities are significantly higher. While inherent risks are common in mainframe operating systems, most enterprises have a limited formal approach to the identification and remediation of such risks. Vulnerabilities, in turn, make mainframe operating systems a major target for cyberattacks with far-reaching financial and company reputation implications.

Security is paramount in financial institutions where personal and financial data processing and transactions are at risk of hacking. In order to limit unauthorized access and protect data, mainframes apply multiple security measures such as encryption, access authorization, logging, and intrusion detection [2]. Security solutions based on mainframe capabilities can help financial institutions meet compliance requirements. Mainframes use a multi-layered security system to protect confidential information and important operations in the banking sector [3]. Such control measures include the use of role-based access control measures as well as highly defined permission control measures. Data encryption is widely applied to secure data, thereby safeguarding confidentiality and integrity [1]. Other enhanced authentication techniques, like multi-factor and biometrics, also offer an extra layer of protection as they confirm the user's identity [1]. Thus far, the evidence reviewed has demonstrated that mainframes tend to have separate hardware security modules for processing secure keys and other cryptography-related tasks in financial institutions.

Mainframes consist of proprietary operating systems that have security built into the fundamental structure of the platform. The operating systems are designed in a manner that can reduce the risks of being compromised and create a robust security status [21]. The operating systems use security mechanisms, including mandatory access control, which enables precise regulation of resource access and data manipulation. The operating systems in mainframes contain thread-security features [9]. Similarly, the mainframe computing platforms have extensive auditing and logging features to provide the essentials of monitoring and compliance. Each activity of a user log-in, data access, or modification to the system is recorded, giving an account of events, thereby establishing effective security features [4]. The audit trail has a significant role in security investigation purposes, compliance, regulatory guidelines, and controls.

Mainframes are known to be reliable and highly available computing platforms. Mainframes enhance availability by meeting demands with high availability and limited disruption [8]. As a result of redundancy and failover characteristics of mainframes, financial institutions can continue providing service in the event of a breakdown or disasters of hardware [16]. Mainframes also use features like parallelism and workload to provide efficient system performance and resource consumption. Mainframe parallel processing makes it possible for most mainframes to divide large tasks into smaller sub-tasks where several processors can perform tasks at the same time, hence making mainframes effective in handling large amounts of data [14]. Complex workload management automatically allocates resources based on priority and necessity to ensure that crucial financial transactions are allocated adequate resources. Mainframes maintain their popularity due to their flexibility, compatibility with virtualization, and integration with progressive technologies. They are reliable and dependable technology that financial institutions rely on even in complex situations [14].

Mainframes have advanced capability of error detection and correction to minimize data corruption and system failure. Mainframes use reliable methods like error-correcting code and parity checks to help detect and correct any errors that may occur during data transmission and storage [15]. Mainframes also have an array of features in hardware redundancy and fault tolerance to enable financial institutions' systems to operate even in case of hardware failures [22]. Similarly, mainframe vendors are equally involved in longterm reliability through timely service and upgrades [5]. The updates restore possible risks, correct logical flaws in the programs, and include optimizations and additional options.

Mainframes are highly scalable and can accommodate growing transaction volumes and data processing needs in financial institutions. Financial institutions can scale up processing power, memory, or storage as needed to facilitate corporate growth and expansion [7]. Mainframes also support virtualization, which means that resources are used optimally, and many tasks can be run on a single mainframe. Mainframes offer enhanced virtualization features that can help allocate resources optimally and manage diverse workloads within a single system [11]. By using multiple virtual environments, banks can have several applications and different workloads on the same physical infrastructure, which helps to save money on hardware acquisition. The virtualization ability adds to the scalability and flexibility of mainframe systems to address changing business requirements effectively [13]. Thus, mainframes' outstanding scalability enables financial institutions to address increasing numbers of transactions and data processing requirements most efficiently and cost-effectively possible.

The security and reliability of the mainframe remain a key asset to business enterprises. The mainframe is one of the most important information technology infrastructures, accounting for at least 71% of organizations' assets [14]. With this role, the mainframe is typically used to guarantee efficient and effective execution of business activities, such as sending key data required by modern technologies like machine learning and artificial intelligence for decision-making processes [17]. Cyber-attacks against mainframes have increased as their importance in business becomes invaluable. The common areas of cyberattack include lost or stolen credentials, which are inherently composed of a user's identity attributes (first name, last name, ID, email, username, password, and in some cases, social security number) and have been the single most common security attack for hackers to access an organization's critical data, web application, and infrastructure (e.g., servers and databases) [8]. HelpNet Security states that mainframe security is a top priority for 85% of IT professionals, yet few are adequately protecting their systems [15].

Despite the extensive research on mainframe security and reliability, there are still gaps that need to be addressed [23]. Specifically, there is a lack of comprehensive studies on the effectiveness of new security technologies and the long-term impact of cloud integration on mainframe reliability [19]. This study aims to fill these gaps by providing updated data and insights into these areas.

2. Research Method

A quantitative methodology was adopted to conduct this study. Quantitative methods are used when the researcher purposed to collect and analyze numerical data [12]. Analyzing numerical data is a key strength of quantitative studies as they improve the generalizability, validity, and reliability of the study findings. Therefore, a quantitative study was justified because the purpose of this study was to collect and analyze quantitative data related to the security and reliability of mainframes in financial institutions [6]. A qualitative methodology was applied to provide an in-depth analysis of security incidents in mainframe systems. A quantitative descriptive study design was adopted to guide data collection and analysis. A descriptive research design was selected because the focus of the study was to gather quantifiable data to statistically analyze a population sample [6]. In turn, the statistical data collected and analyzed can show patterns, connections, and trends over time [12]. The research was designed to collect and analyze data from multiple financial institutions regarding security incidents and the reliability of mainframes.

Secondary data was used in this study. Data were retrieved from industry reports, financial institution case studies, and security incidents. The databases used were IBM XForce Exchange and Verizon Data Breach Investigations Report (DBIR). IBM X-Force

Exchange was used to extract Key metrics such as number of incidents, types of threats (e.g., malware, insider threats, external hacking), and the severity of these threats. The databases provide detailed information relating to security incidents and mainframe reliability metrics.
Quantitative data were analyzed using statistical methods to identify trends and patterns in mainframe security and reliability. An Excel file was used to group the incidence and calculate the mean, frequency, and other statistical measures. Using the data retrieved from IBM X-Force Exchange and DBIR, the common security threats to mainframes in financial institutions were identified. The analysis of this data was through the frequency, severity, and impact of various threats. DBIR provided insights into data breaches and security incidents across various industries, including finance. Major metrics were incident frequency, attack vectors, threat actors, and data compromise. Another key area related to the analysis of mainframe reliability metrics. Analysis of reliability metrics focused on uptime, failure rates, and recovery times. Finally, a comparison of the reliability metrics across different financial institutions was conducted to identify best practices and areas for improvement.

3. Results and Analysis

3.1 Results

The analysis of data collected from IBM X-Force Exchange and Verizon Data Breach Investigations Report (DBIR) provides a comprehensive view of the security threats, mitigation strategies, and reliability of mainframes in financial institutions. This section details the key findings from the data analysis, addressing the research questions posed in this study. The data revealed a significant number of security incidents affecting mainframes in financial institutions. Across the five financial institutions analyzed, a total of 338 security incidents were reported. These incidents were categorized as follows:
Malware Incidents: 204 incidents (60.4%), Insider Threats: 36 incidents (10.7%), and

External Attacks: 98 incidents (29.0%). Malware incidents were the most prevalent, accounting for over 60% of the total incidents. Insider threats and external attacks also posed substantial risks, highlighting the diverse range of threats faced by mainframes in the financial sector. A summary is presented in Table 1 below.

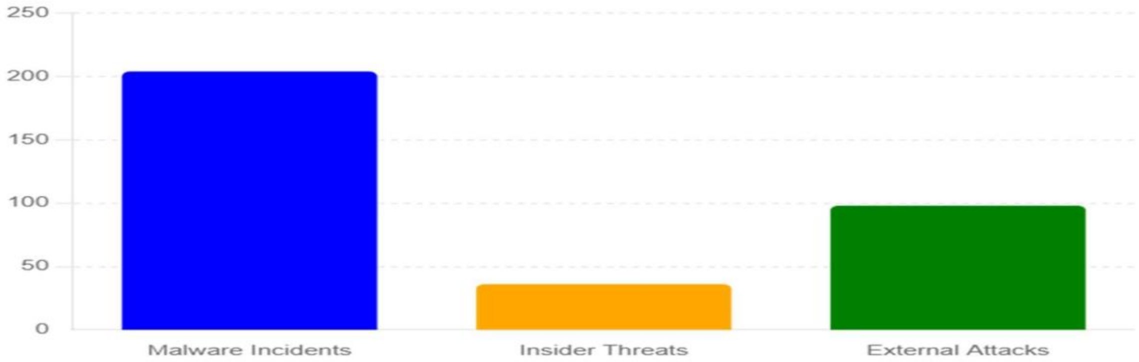


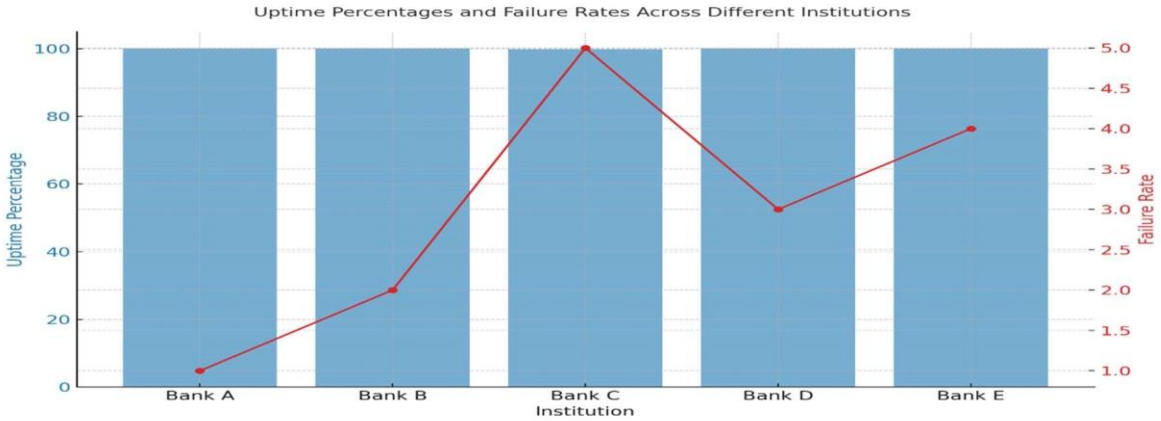
Table 1. Distribution Of Threat Types In Financial Institutions

Note: Y-axis (Number of Incidents by; X-axis (Threat Type)

International Journal of Engineering & Scientific Research
Vol.13 Issue 01, January 2025
ISSN: 2347-6532 Impact Factor: 8.076
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

An analysis was conducted to determine the uptime percentages, failure rates, and recovery times. Based on the findings, the average uptime percentage is 99.97%, demonstrating the high reliability of mainframe systems for the financial institutions studied. On the other hand, institutions experienced 3 failures on average, indicating robust system performance but also room for improvement. The average recovery time following an incident was 3 hours, suggesting that while systems are generally reliable, the recovery process can still be optimized. A summary is shown in Table 2 below.

Table 2. Uptime percentage and failure rates Across different institutions



International journal of Management, IT and Engineering

Data from the Verizon DBIR was used to provide insights into the frequency and impact of data breaches. The analysis revealed that the five banking institutions reported a total of 25 data breaches. Consequently, the breaches caused a variation in downtime, with an average of 10.8 hours per institution. The financial impact of the breaches was $2,500,000, with considerable variations across the banking institutions. The results also indicated that financial loss per hour of downtime was not constant, suggesting different levels of resilience of breach mitigation strategies, as shown in Table 3.

Table 3. Summary of the Analysis

Institution	Malware Incidents	Insider Threats	External Attacks	Uptime Percentage	Failure Rate	Recovery Time (hours)	Data Breaches	Downtime Due to Breach (hours)	Financial loss Due to Breach ($)	Total Security Incidents	Impact Score
Bank A	45	10	20	99.99	1	1	5	10	500000	75	50000
Bank B	32	5	15	99.98	2	2	3	8	300000	52	37500
Bank C	50	8	25	99.95	5	5	7	15	700000	83	46666.667
Bank D	47	6	18	99.97	3	3	6	12	600000	71	50000
Bank E	30	7	20	99.96	4	4	4	9	400000	57	44444.444

3.2 Analysis

The findings provided crucial insights relating to the security and reliability of mainframes in financial institutions. Based on the findings, although existing security measures could be considered effective, there are still certain areas where improvements are needed to guarantee the reliability of mainframes and their stability from cyber threats.

The findings indicated a high rate of malware in mainframe systems. Technically, the increased risk of malware incidents underlines the need to implement continuous monitoring security protocol in mainframes, including conducting regular updates to the system. Based on the findings, there is a need for stakeholders in financial institutions to remain cautious and proactive when designing and implementing malware mitigation strategies for mainframe systems. The findings also underscored the cost and common causes of malware and threats. As per the findings, it was established that insider threats, although less often, could potentially pose a considerable cybersecurity risk attributed to the potential access or knowledge owned by the firm insiders, including employees [18]. The findings also underlined the growing risk of external attacks on mainframe systems. Consequently, it is important to note that external attacks may continue to be a key threat, necessitating wideranging security measures to protect against sophisticated cybercriminal tactics targeting the mainframe [15].

The study findings indicated a high uptime in mainframe systems. Given the findings, the high average uptime percentage (99.97%, Table 3) and relatively low failure rate (3) demonstrate that existing mitigation strategies could be dependable in guaranteeing the reliability of mainframe systems within financial institutions. Findings suggest that conducting regular security audits, timely software updates, and advanced authentication may improve the reliability of mainframe systems by reducing the risk impact of cyberattacks. However, the average recovery time of 3 hours, as per the findings, underscores the idea that this is an area that requires further and regular improvement [15]. As explained and supported by cite, reducing recovery times by leaders in organizations is key to minimizing the impact of incidents and maintaining uninterrupted operations of the mainframe systems [7]. In view of the current study findings, the following recommendations are suggested to promote the security and reliability of mainframes in financial institutions. There is a need to increase monitoring of the mainframe systems, including retaining an incidence response. The process could include leaders implementing highly advanced and sophisticated real-time system monitoring tools for early detection and response to security threats that could undermine the reliability of the mainframe systems [12].

One of the key sources of risks to the mainframe identified in this study was insiders. In this regard, it is suggested that the organization leaders implement strategies that could strengthen the insiders' threat management knowledge. The approach could include regular cyber threat training and risk awareness programs about the potential risks and mitigation approaches for each risk identified. There is also a need to limit insiders' access to sensitive information. This study has several limitations, including the reliance on data from a limited number of financial institutions and the potential variability in reporting standards between institutions. The study solely used secondary data, which could have been subject to longitudinal effects. Future research should aim to include a wider range of institutions and explore the long-term impact of emerging security technologies on mainframe reliability.

4. Conclusion

The security and reliability of mainframes in financial institutions are critical to maintaining the integrity and confidentiality of financial operations. While existing measures may be effective, there is always an opportunity for system improvement, given the increasing complexity of cyber risks. By enhancing monitoring, strengthening insider threat management, investing in advanced technologies, optimizing recovery protocols, and conducting regular audits, financial institutions can further bolster the security and reliability of their mainframe systems. These improvements will help ensure that mainframes continue to serve as a robust backbone for financial operations in an increasingly digital world.

Reference

[1] Abbas, Y. K. (2024). Reflection of cloud computing on improving financial accounting system: An analytical study of opinions of a sample of employees in commercial banks. World Economics and Finance Bulletin, 30,
162-169. https://scholarexpress.net/index.php/wefb/article/view/3722

[2] Akhtar, Z. B. (2024). Securing operating systems (os): A comprehensive approach to security with best practices and techniques. International Journal of Advanced Network, Monitoring and Controls, 9(1), 100-111.
https://doi.org/10.2478/ijanmc-2024-0010

[3] Alevizos, L., & Stavrou, E. (2023). Cyber threat modeling for protecting the crown jewels in the Financial Services Sector (FSS). Information Security Journal: A Global Perspective, 32(2), 134-161.
https://doi.org/10.1080/19393555.2022.2104766

[4] Ang'udi, J. J. (2023). Security challenges in cloud computing: A comprehensive analysis. World Journal of Advanced Engineering Technology and Sciences, 10(2), 155-181. https://doi.org/10.30574/wjaets.2023.10.2.0304

[5] Bhasin, A., & Tripathi, M. (2021). Quantum computing at an inflection point: Are we ready for a new paradigm. IEEE Transactions on Engineering Management, 70(7), 2546-2557.
https://doi.org/10.1109/TEM.2021.3103904

[6] Edler, L., Poirier, K., Dourson, M., Kleiner, J., Mileson, B., Nordmann, H., ... & Würtzen, G. (2002).
Mathematical modelling and quantitative methods. Food and Chemical Toxicology, 40(2-3), 283-326.

[7] Farrow, G. S. (2020). Open banking: The rise of the cloud platform. Journal of payments strategy & systems, 14(2), 128-146. https://www.ingentaconnect.com/content/hsp/jpss/2020/00000014/00000002/art00006

[8] Gazzola, V., Menoni, S., Ghignatti, P., Marini, A., Mauri, R., & Oldani, G. (2023). Analysis of territorial risks and protection factors for the business continuity of data centers. Sustainability, 15(7), 1-24.
https://doi.org/10.3390/su15076005

[9] Islam, R., Patamsetti, V., Gadhi, A., Gondu, R. M., Bandaru, C. M., Kesani, S. C., & Abiona, O. (2023). The future of cloud computing: Benefits and challenges. International Journal of Communications, Network and
System Sciences, 16(4), 53-65. https://doi.org/10.4236/ijcns.2023.164004

[10] Khan, D. M., & Mohamudally, N. (2011). From Mainframe to Cloud Computing: A Study of Programming Paradigms with the Evolution of Client-Server Architecture. Journal of Computing, 3(12), 21-27.

[11] Lambropoulos, G., Mitropoulos, S., & Douligeris, C. (2021). Improving business performance by employing virtualization technology: a case study in the financial sector. Computers, 10(4), 52.
https://doi.org/10.3390/computers10040052

[12] Lewin, C. (2005). Elementary quantitative methods. Research methods in the social sciences, 215-225.

[13] Magotra, B., Malhotra, D., & Dogra, A. K. (2023). Adaptive computational solutions to energy efficiency in cloud computing environment using VM consolidation. Archives of Computational Methods in
Engineering, 30(3), 1789-1818. https://link.springer.com/article/10.1007/s11831-022-09852-2#citeas

[14] Malallah, H. S., Qashi, R., Abdulrahman, L. M., Omer, M. A., & Yazdeen, A. A. (2023). Performance analysis of enterprise cloud computing: a review. Journal of Applied Science and Technology Trends, 4(1), 1-12. https://doi.org/10.38094/jastt401139

[15] Markevych, M., & Dawson, M. (2023). A review of enhancing intrusion detection systems for cybersecurity using artificial intelligence (ai). In International conference Knowledge-based Organization 29(3), 30-37. https://doi.org/10.2478/kbo-2023-0072

[16] Nankya, M., Chataut, R., & Akl, R. (2023). Securing industrial control systems: Components, cyber threats, and machine learning-driven defense strategies. Sensors, 23(21), 1-41. https://doi.org/10.3390/s23218840

[17] Norris, D. F., & Kraemer, K. L. (1996). Mainframe and PC computing in American cities: Myths and realities. Public Administration Review, 568-576.

[18] Parr, F., Auerbach, J., & Goldstein, B. (1985). Distributed processing involving personal computers and mainframe hosts. IEEE journal on selected areas in communications, 3(3), 479-489.

[19] Patterson, D. (2018, February). 50 Years of computer architecture: From the mainframe CPU to the domain-specific tpu and the open RISC-V instruction set. In 2018 IEEE International Solid-State Circuits Conference(ISSCC) (pp. 27-31). IEEE.

[20] Rajan, S., & Jairath, A. (2011, June). Cloud computing: The fifth generation of computing. In 2011
International Conference on Communication Systems and Network Technologies (pp. 665-667). IEEE.

[21] Rangaraju, S. (2023). Secure by intelligence: Enhancing products with ai-driven security measures. EPH-
International Journal of Science and Engineering, 9(3), 36-41. https://doi.org/10.53555/ephijse.v9i3.212

[22] Sharma, P., & Prasad, R. (2023). Techniques for implementing fault tolerance in modern software systems to enhance availability, durability, and reliability. Eigenpub Review of Science and Technology, 7(1), 239-251. https://studies.eigenpub.com/index.php/erst/article/view/33

[23] Stoyek, M. R., Hortells, L., & Quinn, T. A. (2021). From mice to mainframes: Experimental models for investigation of the intracardiac nervous system. Journal of Cardiovascular Development and Disease, 8(11), 149.