International Journal of Management, IT & Engineering
Vol. 14 Issue 01, January 2024
ISSN: 2249-0558 Impact Factor: 7.119
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-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Modernizing and securing MainframeApplications in the GenAI Age

Sampath Amatam,
Director, Mainframe Modernization
Avanade Inc, Dallas-USA
Email: Sampath.amatam@gmail.com

Abstract
This article delves into the world of mainframe modernization, exploring the profound impact of Gen AI, security and cybersecurity challenges in the digital age. The author examines how the synergy between mainframes and Gen AI technologies enhances efficiency, automates decision-making processes, and elevates user experiences. Furthermore, the paper underscores the imperative need for robust security measures in mainframe modernization, considering legacy vulnerabilities and regulatory compliance. The paper offers valuable best practices and recommendations for a successful modernization journey. This comprehensive exploration serves as a guidepost for organizations seeking to unlock the potential of their mainframes in the contemporary digital era.

I. Introduction

Although mainframe computers have existed since at least the introduction of the Harvard Mark I in the 1930s, the advent of modern mainframe computing began in 1964 with the introduction of the IBM System/360 computer[*].The IBM 360 was revolutionary because it allowed for compatibility and scalability across a wide range of models and began the standardization of the mainframe architecture.

Today, IBM mainframes host applications that run of many of the world's largest and most successful businesses. An estimated 10,000 mainframe system are being used today for industries spanning banking, healthcare, insurance, retail, telecommunications, travel, and more. Mainframe applications are used to process credit card payments, stock trades, health care claims processing and other business-critical transactions.

Nevertheless, mainframe computing is not without its challenges. Older applications that were originally written decades ago are showing their age, as are the programmers that wrote those applications. COBOL is the standard for mainframe applications, but modern applications are written in newer languages, such as Java.

Furthermore, the widespread adoption of Generative AI (Gen AI) promises significant advances for mainframe modernization efforts. Using Large Language Models (LLMs) and continuous learning it is possible for Gen AI to write and transform actual programming language code, making it possible to modernize applications much more quickly than if coding was done by hand.

Ensuring proper security within mainframe systems is another key aspect of modernization. Mainframe security is a critical concern due to the sensitivity of data and applications they handle. Although mainframe systems are known for their solid security, many mainframe applications were written prior to the wide adoption of the internet and

[*] https://www.ibm.com/ibm/history/exhibits/mainframe/mainframe_PR360.html

connectivity. This can require the adoption of newer security measures to comply with industry and governmental regulations, as well as to address security challenges such as data breaches, insider threats, and unauthorized access.

II. Gen AI in Mainframe Modernization

The complexity inherent in mainframe modernization causes many organizations to be slow to embark on such projects. Recently, however, with the advances being made in Generative Artificial Intelligence (GenAI) which is a subset of Artificial Intelligence (AI), aspects of mainframe modernization efforts are becoming simpler.

But what is GenAI?Simply stated, GenAI is artificial intelligence capable of generating text, images, or other media, using generative models. Generative AI models learn the patterns and structure of their input training data and then generate new data that has similar characteristics. These systems, which rely on machine learning models, particularly deep learning techniques, have made significant advancements in various applications.

One of the most useful types of GenAI for mainframe modernization is Natural Language Generation (NLG) that can generate human-like text. Such capabilities are based on large language models, or LLMs.A large language model is trained on vast amounts of text data to learn the patterns and structures of language, allowing them to perform various natural language processing tasks, such as text generation, translation, summarization, sentiment analysis, and more.LLMs are even capable of generating accurate computer program code. Notable examples of large language models include GPT-3 (Generative Pre-trained Transformer 3)[†], BERT (Bidirectional Encoder Representations from Transformers)[‡], and T5 (Text-to-Text Transfer Transformer)[§].

Large language models are often based on deep neural networks, particularly transformer architectures, which have proven highly effective in modeling sequential data like text. LLMs are trained on datasets that can range from millions to billions of words or documents. The scale of training data helps the model acquire a broad understanding of language.

Large language models are capable of both generating coherent and contextually relevant text and making predictions about language, such as completing sentences or answering questions.Some large language models are designed to understand and generate text in multiple languages, making them versatile for global applications. LLMs are quite versatile, capable of being used in a wide range of applications, from chatbots and virtual assistants to content generation, language translation, summarization, and more.

It is possible to use LLMs to assist in generating computer programming language code generation to provide code snippets, examples, and explanations related to coding. You can describe the problem or task you need help with, and have a relevant program generated based on your description. Or convert from one programming language to another.

One example of software that uses GenAI to modernize legacy applications is IBM's recently announced Watsonx.ai[**]. Delivered in May 2023, IBM Watsonx.ai is an AI platform consisting of multiple components and a set of AI assistants that can help your modernization project.

The AI studio of watsonx.ai delivers foundation models, training and tuning tools, and an infrastructure for their usage. The foundation model library provided by IBMuse a large, curated set of enterprise data, trained not just on language, but on a variety of areas,

[†] https://www.techtarget.com/searchenterpriseai/definition/GPT-3
[‡] https://blog.research.google/2018/11/open-sourcing-bert-state-of-art-pre.html
[§] https://github.com/google-research/text-to-text-transfer-transformer
[**] https://newsroom.ibm.com/2023-05-09-IBM-Unveils-the-Watsonx-Platform-to-Power-Next-Generation-Foundation-Models-for-Business

including programming language code. Specifically, the fm.code model was designed to enable the automatic generation of code for developers through a natural-language interface.

The watsonx Code Assistant for Z simplifies the task of modernizing COBOL applications. It can be used to incrementally transform COBOL code into well architected high-quality Java code. Such conversion is an important part of legacy application transformation efforts in mainframe modernization projects for several reasons,

As COBOL programmers age and retire, it can be difficult for organizations to hire skilled COBOL programmers capable of maintaining and supporting existing COBOL code. COBOL and procedural coding are not taught at most universities any longer. However, finding programmers with Java skills is easy as Java is taught as the primary programming language in most universities and trade school programs.

Another key reason organizations consider moving from COBOL to Java is to reduce cost. According to a recent survey by BMC Software "a typical company's overall mainframe budget (is) increasing annually by 5 percent to 11 percent."†† And a large part of this cost is accrued by software cost. Converting COBOL program to Java can have reduce software costs. How this is achieved is covered in Section IV of this paper, "The Impact and Benefits of Mainframe Specialty Processors."

Although GenAI can be useful for code-related tasks, it is not a complete replacement for experienced software developers. One must still review and test the code generated by software that uses LLMs (such as watsonx.ai) to verify its accuracy and viability. Additionally, programming context, best practices, and specific libraries or frameworks may change over time, so it's a good idea to verify the code against up-to-date resources.

Nevertheless, GenAI models have significantly advanced the state of the art in natural language understanding and generation. And they can be useful to optimize mainframe modernization projects, making possible many heretofore impossible or difficult tasks.

III. Security and Cybersecurity in Mainframe Modernization

Robust security is necessary for a mainframe computing environment because of the mission critical workloads that run on the platform. Mainframes were among the first large-scale computing systems used by businesses, government organizations, and academic institutions. As such, security has been a priority for mainframe systems almost from the start. However, security concerns were different from modern ones due to the limited technology and different computing environment.

Early mainframes were typically isolated computing systems with limited or no external network connectivity. This isolation provided a degree of inherent security, as there were fewer entry points for attackers. Security breaches typically involved physical access to the mainframe's location. However, modern mainframes are networked and integrated into the fabric of the Internet, exposing them to all types of security issues that modernization projects must address.

Early mainframes used basic authentication mechanisms, such as usernames and passwords. This provides a solid foundation for protecting the mainframe environment because arguably the most important thing in security is identity. However, password management and encryption were not as advanced as they are today, making them more vulnerable to insider threats and brute-force attacks. Modernizing authentication practices for mainframes can include:

†† BMC Software, "Deliver Better Results for Mainframe Cost Reduction Initiatives," https://www.bmc.com/documents/white-papers/better-results-for-maunframe-cost-reduction.html

- **Multi-Factor Authentication (MFA)** requiring users to provide two or more authentication factors before they can access a system. Common factors include something you know (password), something you have (a mobile device or smart card), and something you are (biometric data like fingerprints or facial recognition). MFA significantly increases security by adding layers of protection.

- **Single Sign-On (SSO)**, a convenience-oriented authentication method, allows users to access multiple applications and systems with a single set of credentials. While it simplifies user experience, it can also enhance security by centralizing authentication and reducing the need for users to remember multiple passwords.

- **Mainframes can deploy biometric data**, such as fingerprints, iris scans, or facial recognition, to authenticate users. Biometric authentication offers a high level of security because it relies on unique physical characteristics.

- **Smart cards and tokens** can be used that generate time-based or one-time passwords for authentication. These physical devices add an extra layer of security and are particularly useful in highly secure environments.

Other forms of modern authentication that can be adopted during a mainframe modernization project include password-less authentication, client certificates, federated authentication, and behavioral and contextual authentication that analyzes the user's behavior patterns, such as typing speed and keystroke dynamics, to determine their identity.

When a platform has existed for more than a half Century, there will have been many changes to not only computing standards and protocols, but to user expectations and requirements as well. In their earliest days mainframes primarily processed batch jobs, which meant that users submitted their work in batches, and it was processed sequentially. This limited real-time interactions and reduced the potential for online security threats. Indeed, early mainframes operated in a pre-Internet era, which meant they were not exposed to the wide range of internet-based attacks we see today.

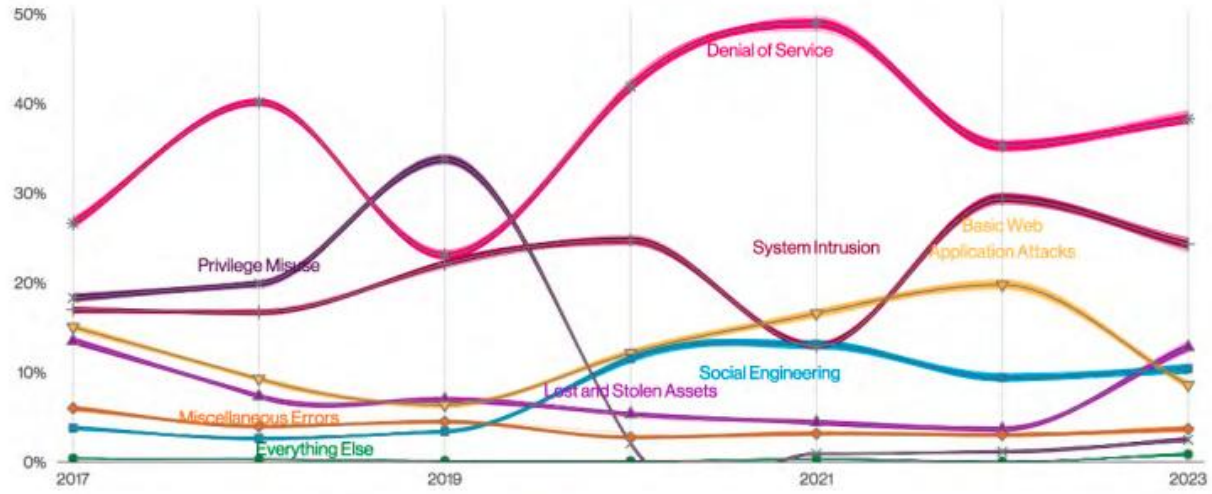
Remote access to mainframes was practically non-existent in the early days. Users had to be physically present at the mainframe facility to interact with the system. Even as late as the 1980s specialty machines were required to work on a mainframe remotely that would require the mainframe to be pinged and then call back the machine at a specific location.

The concept of computer viruses and malware, as we know them today, did not exist in the early mainframe era. Security threats were more likely to come from insiders with physical access.

Another limiting factor in the age of the early mainframe was that privilege separation was not as well-defined as in modern systems. A user with access to the system often had significant control over the entire system. And data encryption was not commonly used, so sensitive data was often protected through physical security and access controls rather than cryptographic methods.

As technology evolved, mainframe security measures also evolved to address the changing threat landscape. Today, modern mainframe security incorporates advanced authentication, encryption, access control, audit trails, and protection against a wide range of cyber threats. While the security landscape has become more complex, the principles of early mainframe security, such as physical security and controlled access, remain important components of a comprehensive security strategy for modern mainframes.

Furthermore, exposing the mainframe to the Internet opens up the platform for data breach attacks. A data breach is a security incident that results in unauthorized access to confidential information.One can quickly come to grips with the variety and patterns of attacks by reviewing the patterns over time in security incidents as published in the Verizon 2023 Data Breach Investigations Report[‡‡].



Patterns over time in incidents (Source: Verizon 2023 Data Breach Investigations Report)

Surely it becomes obvious that a simple Userid and password is insufficient to protect against so many types of attacks. Techniques that can be deployed as part of a mainframe modernization project to bolster security against data breach attacks include:

- **Data Encryption:** Modernization efforts should prioritize data encryption both in transit and at rest. Advanced encryption algorithms and key management are essential for protecting sensitive data.

- **Vulnerability Management:** Regularly scan and assess the mainframe environment for vulnerabilities. Address any identified security weaknesses promptly and apply patches or updates as necessary.

- **Security Monitoring:** Implement robust security monitoring and auditing mechanisms to detect and respond to any suspicious or unauthorized activities. This includes the use of intrusion detection systems and SIEM (Security Information and Event Management) solutions.

[‡‡]https://www.verizon.com/business/resources/reports/dbir/

- **Secure Development Practices:** Ensure that modernization efforts follow secure development practices to prevent vulnerabilities in new applications or updated software. One such approach is advocated by the DevSecOps[§§]approach which advocates embedding security at every phase of the software development lifecycle.

- Education and Training: Provide ongoing education and training to staff responsible for mainframe security to keep them informed about the latest threats and security best practices.

Finally, compliance needs to be a significant focus of the mainframe modernization effort. Compliance refers to the adherence to specific laws, regulations, standards, and industry best practices that are relevant to an organization's operations and the handling of data. In the context of mainframe modernization, compliance plays a significant role in several ways.

Many industries and regions have established regulations that govern data security, privacy, and IT practices. Examples include HIPAA (healthcare)[***], PCI DSS (payment card industry)[†††], GDPR (General Data Protection Regulation)[‡‡‡], SOX (Sarbanes-Oxley)[§§§],and various financial industry regulations. Mainframe modernization efforts must ensure that the new and revised systems comply with all relevant regulations, especially regarding how to handle sensitive data.

Data privacy laws, such as GDPR and the California Consumer Privacy Act (CCPA)[****], place strict requirements on how personal data is collected, processed, and protected. Compliance with these regulations is crucial when handling customer data during mainframe modernization.

Compliance may also involve adhering to industry-specific security standards, such as ISO 27001[††††] or NIST SP 800-53[‡‡‡‡]. These standards provide guidelines and best practices for information security, risk management, and data protection.

Of course, there are many additional aspects of compliance that need to be incorporated into mainframe modernization efforts including understanding a complying with internal policies and procedures, conducting effective audits, risk mitigation, and most importantly, data classification. Compliance requires that data be effectively classified based on its sensitivity and importance. During modernization, it's essential to correctly identify and protect data based on its classification.

Modernizing mainframes and the software that runs on them can enhance their security posture, but it's essential to ensure that the modernization efforts include robust security measures. Regular updates, a focus on data protection, and adherence to best practices can help organizations maintain a strong security posture in their mainframe environments.

[§§] https://www.techtarget.com/searchitoperations/definition/DevSecOps
[***] https://www.hhs.gov/hipaa/index.html
[†††] https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf
[‡‡‡] https://gdpr-info.eu/
[§§§] https://sarbanes-oxley-act.com/
[****] https://oag.ca.gov/privacy/ccpa
[††††] https://www.iso.org/standard/27001
[‡‡‡‡] https://www.nist.gov/privacy-framework/nist-sp-800-53

IV. Conclusion

As organizations that rely on the IBM mainframe for its power, scalability, and reliability work on integrating modern technologies and architectures into their IT fabric they are embarking on initiatives to modernize their mainframe systems. Such projects can be challenging because mainframe systems are responsible for running the infrastructure of some of the largest businesses on the planet.

This article has reviewed and examined several technologies that can help organizations succeed when modernizing their mainframe systems and applications. By embracing Gen AI capabilities organizations can more readily convert aging applications to a more modern language. Furthermore, modernization projects can tackle security and cybersecurity challenges by applying newer technologies to better protect mainframe applications as they are exposed to threats were not initially designedto be protected from.

V. References

Hudson, Andrew. The IBM Mainframe: How it runs and why it survives. (ARS Technica, 2023). https://arstechnica.com/information-technology/2023/07/the-ibm-mainframe-how-it-runs-and-why-it-survives/

IBM System/360 Announcement Letter. (Press release, 1964). https://www.ibm.com/ibm/history/exhibits/mainframe/mainframe_PR360.html

Loomis, Skyla, et al. Accelerate Mainframe Application Modernization with Hybrid Cloud. (IBM Redbook, 2023). ISBN 978-0738461090

Lascu, Oactvian, et al. IBM z16 Technical Introduction. (IBM Redbook, 2023). ISBN 978-0738461083

Lascu, Oactvian, et al. IBM z16 (3931) Technical Guide. (IBM Redbook, 2022). ISBN 978-0738460789

Tozzi, Christopher. 10 Mainframe Statistics That May Surprise You. (Precisely, 2022). https://www.precisely.com/blog/mainframe/9-mainframe-statistics