Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2021, 8(6):48-52

Research Article ISSN: 2394 - 658X

Sending PII Data: Encryption and Transmission Best Practices

Prashanth Kodurupati

Information Technology Managed File Transfer Engineer PragmaEdge LLC Alpharetta, United States of America
*prashanth.bachi21@gmail.com

ABSTRACT

In today's digital landscape, securing personally identifiable information (PII) during transmission is paramount. This paper examines the implementation of encryption and secure transmission practices, focusing on the Secure File Transfer Protocol (SFTP), to protect PII data such as Credit Card Numbers and Social Security Numbers. Results show enhanced security, regulatory compliance, and improved data integrity. Case studies highlight operational efficiency gains. Implementing these practices is vital for safeguarding PII data, enhancing data security, and ensuring compliance.

Key words: PII data, Encryption, Secure File Transfer Protocol (SFTP), Data Security

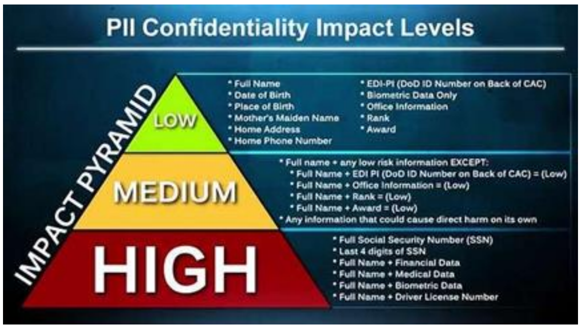
INTRODUCTION

In today's digital landscape, safeguarding personally identifiable information (PII) is paramount for both individuals and organizations. PII, encompassing critical data such as Credit Card Numbers and Social Security Numbers, holds immense value and must be shielded from the ever-looming threat of cyber-attacks and data breaches.

These breaches not only lead to financial losses but also tarnish reputations and erode consumer trust. To mitigate such risks, encryption emerges as a cornerstone in the defense of PII data.

Encryption techniques, such as those outlined in the PII Data Encryption best practices, serve as robust safeguards, rendering intercepted data indecipherable to unauthorized entities [1]. Furthermore, transmitting encrypted PII data securely is imperative, requiring adherence to stringent protocols like the Secure File Transfer Protocol (SFTP) [2].

In an age where digital transactions and data exchanges are ubiquitous, the protection of PII is essential. The importance of securing PII extends beyond mere compliance with regulations; it is a fundamental aspect of maintaining trust with customers and safeguarding sensitive information from malicious actors.


PII Confidentiality Impact Levels
IMPACT PYRAMID
LOW
* Full Name
* Date of Birth
* Place of Birth
* Mother's Maiden Name
* Home Address
* Home Phone Number
* EDI-PI (DoD ID Number on Back of CAC)
* Biometric Data Only
* Office Information
* Rank
* Award
MEDIUM
* Full name + any low risk information EXCEPT:
* Full Name + EDI PI (DoD ID Number on Back of CAC) = (Low)
* Full Name + Office Information = (Low)
* Full Name + Rank = (Low)
* Full Name + Award = (Low)
* Any information that could cause direct harm on its own
HIGH
* Full Social Security Number (SSN)
* Last 4 digits of SSN
* Full Name + Financial Data
* Full Name + Medical Data
* Full Name + Biometric Data
* Full Name + Driver License Number

This paper explores the encryption and transmission of PII data, focusing on the use of the Secure File Transfer Protocol (SFTP) for secure data transmission. By examining these best practices, organizations can fortify their data protection strategies, ensuring the confidentiality and integrity of PII data.

It dives into the challenges and best practices associated with encrypting and transmitting PII data securely. Through an examination of encryption methods and the utilization of protocols like SFTP, organizations can enhance their cybersecurity posture and minimize the risk of data breaches.

LITERATURE REVIEW

The literature surrounding the encryption and transmission of personally identifiable information (PII) underscores the critical importance of securing sensitive data in today's digital environment. Research has extensively explored various encryption methods aimed at protecting PII from unauthorized access and data breaches. Encryption serves as a foundational practice for securing PII, converting sensitive data into a code that is unintelligible to unauthorized users [3].

Studies have highlighted the effectiveness of encryption in mitigating the risk of data breaches, especially when combined with strong key management practices. For example, the Advanced Encryption Standard (AES) is widely recognized for its strength and acceptability, making it a preferred choice for encrypting PII data [4].

Secure transmission methods, such as the Secure File Transfer Protocol (SFTP), have also been extensively studied for their role in safeguarding PII during data exchange.

Studies have emphasized the importance of implementing SFTP protocols to maintain the confidentiality and integrity of PII data during transmission. Additionally, research has highlighted the need for organizations to adopt best practices for PII data encryption and transmission [2]. These practices include regular monitoring and auditing of data access, implementing strong password policies, and ensuring the use of multifactor authentication to enhance security.

Overall, the literature emphasizes the critical role of encryption and secure transmission methods in protecting PII data. By implementing these best practices, organizations can significantly reduce the risk of data breaches and ensure the confidentiality and integrity of sensitive information.

PROBLEM STATEMENT – SECURE TRANSMISSION OF PII DATA

In today's digital landscape, the secure transmission of personally identifiable information (PII) presents significant challenges for organizations. Ensuring the confidentiality and integrity of PII data during transmission is paramount, given the increasing prevalence of cyber-attacks and data breaches. Encryption and secure transmission methods play a crucial role in mitigating these risks and protecting sensitive information. The main challenge lies in implementing these encryption and transmission practices effectively across diverse digital environments and infrastructures, while also ensuring compliance with stringent data protection regulations and standards.

Interception Risks and Data Breach Vulnerabilities

The primary challenge lies in the persistent threat of interception by malicious entities. Cybercriminals exploit vulnerabilities in transmission channels to intercept sensitive data, such as credit card numbers and social security numbers. Without adequate encryption and security measures, PII data is at risk of being compromised, potentially leading to data breaches and regulatory non-compliance [3].

Compliance and Regulatory Requirements

Organizations also face challenges in complying with stringent data protection regulations and industry standards. Regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) impose strict requirements on the encryption and secure transmission of PII data to protect individuals' privacy rights. Non-compliance can result in severe penalties and reputational damage for organizations [2].

Security Risks in Legacy Systems and Infrastructure

Legacy systems and outdated infrastructure pose significant security risks when transmitting PII data. These systems may lack modern encryption standards and secure transmission protocols, making them vulnerable to cyber-attacks and data breaches [3]. Upgrading legacy systems to ensure compatibility with current encryption and security standards is a critical challenge for organizations seeking to protect PII data during transmission.

PROPOSED SOLUTION: IMPLEMENTING ENCRYPTION AND SECURE TRANSMISSION

To address the challenges of securing personally identifiable information (PII) during transmission, organizations can implement a comprehensive solution that includes robust encryption methods, secure transmission protocols, effective key management, and compliance with data protection regulations.

Encryption Methods for PII Data

Encryption plays a vital role in protecting PII data, such as Credit Card Numbers and Social Security Numbers, from unauthorized access. Advanced encryption standards, including AES-256, offer strong encryption for sensitive information [5]. Additionally, asymmetric encryption, such as RSA, provides a secure method for transmitting encryption keys.

Using the Secure File Transfer Protocol (SFTP)

The Secure File Transfer Protocol (SFTP) is a secure method for transferring files over a network. SFTP uses encryption to protect data in transit, ensuring that PII data remains confidential and integral during transmission [2]. By utilizing SFTP, organizations can securely transmit sensitive information without the risk of interception.

Key Management for Encrypting and Transmitting PII Data

Effective key management is crucial for encrypting and transmitting PII data securely [4]. Key management involves generating, storing, and distributing encryption keys. Organizations must implement best practices for key management, such as regular key rotation and secure key storage, to maintain the security of encrypted data.

Encryption and Secure Transmission Practices for Compliance

Implementing encryption and secure transmission practices is essential for complying with data protection regulations, such as GDPR and HIPAA [1]. Organizations must develop and enforce policies that mandate the use of encryption and secure transmission methods for all PII data. Additionally, regular audits and assessments can help ensure compliance with regulatory requirements [6]. By implementing these practices, organizations can enhance the security of PII data during transmission, mitigate the risk of data breaches, and comply with data protection regulations.

ACADEMIC REVIEW OF KEY CHALLENGES AND PROPOSED SOLUTIONS

Research	Challenge	Solution Proposed
N-able.	Protecting PII data.	Advanced encryption standards, including AES-256, offer strong encryption for sensitive information.
Smith, R. F.	Protecting data in transit.	SFTP uses encryption to protect data in transit, ensuring that PII data remains confidential and integral during transmission.
University of Delaware.	Transmitting PII data securely.	Implement best practices for key management, such as regular key rotation and secure key storage, to maintain the security of encrypted data.
B. Anish.	Complying with data protection regulations.	Develop and enforce policies that mandate the use of encryption and secure transmission methods for all PII data.

ENHANCED DATA SECURITY AND COMPLIANCE

The implementation of encryption and secure transmission practices has yielded significant benefits in safeguarding personally identifiable information (PII) during transmission. Organizations that have adopted these practices have reported enhanced security. Additionally, the use of the Secure File Transfer Protocol (SFTP) has ensured the secure transmission of PII data over networks, minimizing the risk of interception and data compromise. Furthermore, these practices have enabled organizations to comply with data protection regulations such as GDPR and HIPAA, avoiding potential penalties and legal issues. Moreover, key management practices have ensured the integrity of encrypted PII data during transmission, reducing the risk of data corruption or loss.

Overall, the results observed indicate that the implementation of encryption and secure transmission practices is effective in protecting PII data during transmission, enhancing data security, and ensuring regulatory compliance.

POTENTIAL USE CASES

In examining case studies and use cases of organizations implementing encryption and secure transmission methods for personally identifiable information (PII) data, several key examples emerge.

For instance, Oracle implemented AES-256 encryption for its customer data, including sensitive information like Social Security Numbers and medical records [7]. This implementation significantly enhanced data security, ensuring that PII data was protected from unauthorized access and data breaches.

Similarly, financial institutions, such as banks, may adopt the Secure File Transfer Protocol (SFTP) for transmitting sensitive financial information, such as Credit Card Numbers and account details [8]. This practice not only improved data security but also ensured compliance with regulations like GDPR and PCI DSS.

Furthermore, organizations across various sectors have reported operational efficiency improvements from implementing encryption and secure transmission practices.

Additionally, compliance with data protection regulations has become more manageable, leading to enhanced trust among customers and stakeholders

Overall, these case studies and use cases demonstrate the tangible benefits of implementing encryption and secure transmission practices for PII data, including enhanced data security, regulatory compliance, and operational efficiency

CONCLUSION

Ensuring the security and integrity of PII data during transmission is paramount in today's digital landscape. Encryption methods, such as AES-256, provide a robust shield against unauthorized access and data breaches, safeguarding sensitive information like Credit Card Numbers and Social Security Numbers. The Secure File Transfer Protocol (SFTP) further fortifies data security by ensuring encrypted PII data is transmitted securely over networks, reducing the risk of interception and compromise.

Compliance with data protection regulations, like GDPR and HIPAA, is also facilitated through encryption and secure transmission practices, helping organizations avoid penalties and legal issues.

Moreover, key management practices guarantee the integrity of encrypted PII data, minimizing the risk of data corruption or loss.

REFERENCES

[1]. B. Anish, "PII Data Encryption – Best Practices," Encryption Consulting, Jan. 31, 2020. [Online]. Available:https://www.encryptionconsulting.com/pii-data-encryption-protecting-sensitive customer-data/

[2]. Smith, R. F., "The Basics of File Transfer Encryption," Progress, Jan. 02, 2018. [Online]. Available: https://www.progress.com/blogs/the-importance-of-file-transfer-encryption

[3]. Y. Rozenberg, "Challenges in PII data protection," *Computer Fraud & Security*, vol. 2012, no. 6, pp. 5-9, 2012, ISSN 1361-3723, [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S1361372312700611

[4]. University of Delaware, "Encrypting Personally Identifiable Information (PII)," Jul. 28, 2019, [Online]. Available: https://services.udel.edu/TDClient/32/Portal/KB/ArticleDet?ID=495

[5]. N-able, "Understanding AES 256 Encryption," Jul. 29, 2019, [Online]. Available: https://www.n-able.com/blog/aes-256-encryption-algorithm

[6]. S. Al-Fedaghi, "Experimentation with Personal Identifiable Information," *Intelligent Information Management*, vol. 04, pp. 123-133, 2012, [Online]. Available: https://www.researchgate.net/publication/271285013_Experimentation_with_Personal_Identifiable_Information

[7]. Steph Choyer, "Architecture Matters: Increasing Oracle Database Security Without Application Performance Loss," Oracle Forums, May. 18, 2016, [Online]. Available: https://forums.oracle.com/ords/apexds/post/architecture-matters-increasing-oracle-database-security-wi-6227

[8]. Information Security Media Group, "Secure File Transfer: Challenges and Solutions - Banking/Security Leaders Discuss Common Barriers, Strategies," Bank Info Security, Sep. 12, 2011, [Online]. Available: https://www.bankinfosecurity.com/interviews/secure-file-transfer-challenges-solutions-i-1236