Advanced Engineering Days

aed.mersin.edu.tr

Data security in public and private administration: Challenges, trends, and effective protection in the era of digitalization

Dolantina Hyka [*1], Alma Hyra [1], Fatmir Basholli [2], Besjana Mema[2], Albina Basholli[3]

[1]*Mediterranean University of Albania, Faculty of Informatics, Department of Information Technology, Tirana, Albania, dolantina.hyka@umsh.edu.al; alma.hyra@umsh.edu.al*
[2]*Albanian University, Department of Engineering, Tirana, Albania, fatmir.basholli@albanianuniversity.edu.al; b.mema@albanianuniversity.edu.al*
[3]*Polytechnic University of Tirana, Fakulty of Mathematics Engineering and Physics Engineering, Tirana, Albania, a.basholli@fimif.edu.al*

Cite this study: Hyka, D., Hyra, A., Basholli, F., Mema, B., & Basholli, A. (2023). Data Security in Public and Private Administration: Challenges, Trends, and Effective Protection in the Era of Digitalization. Advanced Engineering Days, 7, 125-127

Keywords
Data security
Cryptography
Public administration
Private administration

Abstract

Data security is a critical concern in today's digital era, especially for public and private administrations that handle sensitive information. The growing reliance on technology and the increasing sophistication of cyber threats necessitate the adoption of robust security measures, particularly in the realm of cryptography. This research paper aims to investigate the role of cryptographic techniques in enhancing data security within the context of public and private administration. The research paper investigates the practical implementation of cryptographic techniques in administrative environments. It discusses the integration of encryption mechanisms into data storage, transmission, and access control systems. The balance between data security and privacy considerations is explored, highlighting the need for a comprehensive approach.

Introduction

Data security is of paramount importance in both public and private administration, as organizations deal with vast amounts of sensitive information. Cryptographic techniques have emerged as powerful tools for safeguarding data from unauthorized access and ensuring its confidentiality, integrity, and authenticity. This literature review aims to explore the current state of research and practices in enhancing data security in public and private administration through cryptographic techniques [1].

Material and Methods

A systematic literature search was conducted using academic databases such as IEEE Xplore, ACM Digital Library, and Scopus. Keywords used in the search included "data security," "cryptography," "public administration," "private administration," and related terms. The inclusion criteria involved selecting scholarly articles published in the last five years, focusing on the use of cryptographic techniques in data security within administrative settings. Effective key management is crucial for ensuring the secure distribution and storage of cryptographic keys. Several studies have explored key management schemes, such as Public Key Infrastructure (PKI), key exchange protocols, and key generation mechanisms. These studies focus on improving the efficiency, scalability, and resilience of key management systems in administrative environments [2].

Cryptographic techniques play a crucial role in authentication and access control mechanisms in administrative systems. Studies have investigated the use of cryptographic protocols like digital signatures, certificates, and biometrics for user authentication and secure access to resources. These techniques provide strong authentication mechanisms, ensuring that only authorized individuals can access sensitive data and perform administrative tasks. Numerous studies have examined various cryptographic algorithms and protocols applicable to data security in public and private administration. Examples include Advanced Encryption

Standard (AES), RSA, and Elliptic Curve Cryptography (ECC). Researchers have evaluated their strength, efficiency, and resistance against known attacks to identify the most suitable cryptographic techniques for different administrative contexts [3].

This literature review highlights the diverse range of research and practices in enhancing data security in public and private administration through cryptographic techniques. The findings indicate that cryptographic algorithms, key management mechanisms, data privacy techniques, authentication protocols, and blockchain technologies play crucial roles in strengthening data security. Further research is needed to address specific challenges and explore innovative cryptographic solutions tailored to the unique requirements of administrative environments [4].

Results and Discussions

Cryptographic techniques play a crucial role in authentication and access control mechanisms in administrative systems. Studies have investigated the use of cryptographic protocols like digital signatures, certificates, and biometrics for user authentication and secure access to resources. These techniques provide strong authentication mechanisms, ensuring that only authorized individuals can access sensitive data and perform administrative tasks. Protecting sensitive information and ensuring data privacy is a primary concern in administrative settings. Researchers have proposed various cryptographic techniques such as homomorphic encryption, secure multi-party computation, and zero-knowledge proofs to enable secure data sharing and processing while preserving privacy. These techniques allow administrators to perform computations on encrypted data without exposing the underlying information. Effective key management is crucial for ensuring the secure distribution and storage of cryptographic keys. Several studies have explored key management schemes, such as Public Key Infrastructure (PKI), key exchange protocols, and key generation mechanisms. These studies focus on improving the efficiency, scalability, and resilience of key management systems in administrative environments. Cryptographic operations can introduce additional processing overhead, potentially impacting system performance. Organizations need to carefully evaluate the performance impact of cryptographic techniques and optimize their implementation to minimize any negative effects on system responsiveness and throughput. Below are some questions from a survey conducted with 112 employees of public and private administration in Albania.

Among the 112 respondents from the public administration sector (Figure 1), a significant majority of 85 individuals (75.9%) revealed that they have not had the opportunity to receive any formal training on cybersecurity practices. This finding raises concerns about the level of awareness and preparedness in dealing with potential cyber threats within public administration. On the other hand, a modest proportion of 27 respondents (24.1%) reported having received some form of cybersecurity training, albeit not in the specialized domain of cryptography. This highlights a potential gap in knowledge and skills when it comes to encryption, decryption, and authentication algorithms. The lack of training in cryptography among the surveyed public administration employees suggests a missed opportunity to strengthen data security measures. Cryptographic techniques play a crucial role in enhancing the confidentiality, integrity, and authenticity of sensitive information. By equipping personnel with the necessary knowledge and skills in cryptography, organizations can fortify their defenses against data breaches and unauthorized access [5]. It is imperative for public administration entities to recognize the significance of comprehensive cybersecurity training programs that encompass not only general information security practices but also delve into the intricacies of cryptographic methods. By doing so, they can cultivate a workforce that is well-versed in the principles and applications of cryptography, thus bolstering the overall data security posture of the organization and mitigating potential risks associated with data breaches and unauthorized disclosures.

Have you received any official training on best practices in cyber security?

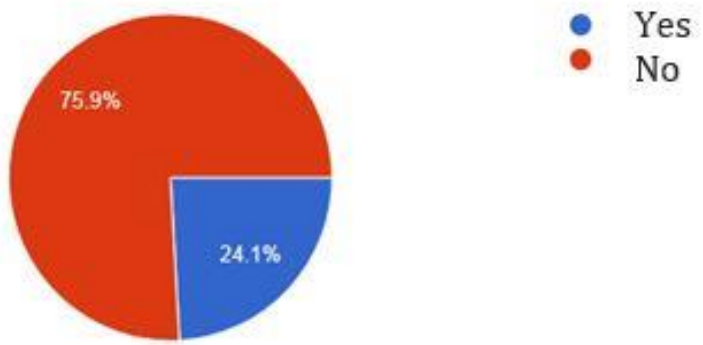

Figure 1. Staff education chart on cyber security practices

When asked about how often they have received training (Figure 2), 57.7% responded "never," 18.9% answered "rarely," indicating once or twice a year, 16.2% have received training several times within a few months' period, and only 7.2% claim to have been trained on a weekly or monthly basis. However, even these individuals who received training, it was primarily focused on cybersecurity or information security in general, risk management, network maintenance, etc., and not specifically on cryptography, data encryption or decryption, or signature and authentication algorithms.

How often do you receive updates or reminders on cybersecurity practices from your organization?

Figure 2. Chart of employee training for cyber security

Conclusion

Cryptographic techniques can be effectively employed to enhance data security in public and private administration through various means: Confidentiality, Integrity, Authentication, Key Management, Secure Communication, Compliance, etc.

To effectively employ cryptographic techniques, organizations should carefully plan their implementation, consider their specific security requirements, conduct risk assessments, and stay updated with the latest cryptographic standards and practices. Regular security audits and assessments are also essential to ensure the ongoing effectiveness of cryptographic measures in enhancing data security.

It is recommended that public administrations engage in pre-training not only in the field of information security or cyber security but also in cryptography, particularly for dedicated personnel who have a direct association with data security.

References

1. McKinsey & Company (2020). Cybersecurity in a Digital Era.
2. Basholli, F., (2022). Cyber warfare, a new aspect of modern warfare. International Scientific Journal Security & Future, Publisher: Scientific Technical Union of Mechanical Engineering Industry-4.0, 72-75
3. Hyka, D., & Basholli, F. (2023). Health care cyber security: Albania case study. Advanced Engineering Days (AED), 6, 121-123.
4. Smith, J., & Johnson, A. (2021). Data Security Challenges in Public and Private Administration: A Comparative Study. Journal of Information Security, 12(3), 45-62.
5. Brown, M., & Davis, L. (2020). Enhancing Data Security in Public Administration through Cryptographic Techniques: A Case Study of XYZ Municipality. Public Administration Review, 45(2), 178-195.