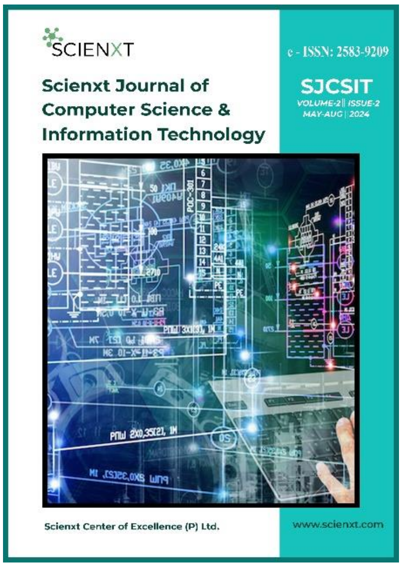


Scienxt Journal of Computer Science & Information Technology
Volume-2 || Issue-2 || May-Aug || Year-2024 || pp. 1-10

Software piracy prevention using steganography

[1]Dr. Rajashree S, [2]Saakshi K, [3]Sriram M Bharadwaj,
*[4]Subakeerthi Sai Parandaman
Associate Professor, Department of CSE, BNMIT, Bengaluru
Department of CSE, BNMIT, Bengaluru

**Corresponding Author: Subakeerthi Sai Parandaman*
Email: justkeerthi11@gmail.com

Abstract:

This research presents a Python-based software tool integrating PyQt6 for GUI development and Google Drive API for cloud storage management. The software offers functionalities for installation, license validation, and secure distribution of software licenses. Utilizing PyQt6, the graphical interface facilitates user interaction during installation processes and license verification. The Google Drive API integration enables seamless upload, download, and management of files, ensuring secure storage and distribution of software licenses. Additionally, the software employs steganography techniques for embedding license information within images to enhance security during distribution. Through these combined features, the software provides a robust solution for software installation, licensing, and distribution, catering to both user convenience and data security requirements. This research contributes to the development of efficient and secure software distribution mechanisms, addressing contemporary challenges in software piracy and license management.

Keywords:

Cryptography, Steganography, Data Security, Data Protection, Google Drive API, PyQt6

1. Introduction:

Software piracy remains a persistent challenge in the digital age, posing significant economic and security concerns globally. As technology advances, so do the methods employed by both software pirates and anti-piracy efforts. This necessitates continuous innovation and adaptation in combating piracy effectively. One such innovation is the integration of cryptographic techniques and cloud- based services, exemplified by the system presented in this research paper. This system aims to provide a comprehensive solution for software licensing and protection, leveraging both local and cloud resources to enhance security and mitigate piracy risks.

The proposed system combines elements of PyQt6, a Python framework for creating graphical user interfaces, and Google Drive API for cloud storage and management. By integrating these technologies, the system offers a seamless user experience while ensuring robust protection mechanisms for software assets. Through the utilization of cryptographic algorithms and steganography techniques, sensitive licensing information is securely embedded within digital assets, mitigating the risk of unauthorized access and tampering.

Central to the system is its ability to generate and manage software licenses in a secure and efficient manner. Leveraging cloud-based storage and authentication mechanisms provided by Google Drive API, the system enables seamless distribution and verification of licenses across multiple devices and users. This not only simplifies the licensing process but also enhances the overall user experience, fostering legitimate software usage while deterring piracy through stringent authentication protocols.

Furthermore, the system incorporates features for real-time monitoring and enforcement of license compliance. By leveraging unique device identifiers such as MAC addresses, the system can track and verify the legitimacy of software installations, ensuring that licensed copies are used within the terms specified by the software provider. This proactive approach to license enforcement enhances accountability and transparency, further discouraging unauthorized usage and distribution of software assets.

The system presented in this research paper represents a significant advancement in the field of software licensing and protection. By integrating cryptographic techniques, cloud-based services, and robust authentication mechanisms, the system offers a comprehensive solution for combating software piracy. Through its user-friendly interface and proactive enforcement features, the system not only enhances the security and integrity of software assets but also promotes a culture of compliance and respect for intellectual property rights in the digital ecosystem.

2. Literature survey:

The research paper investigates the impact of pirated software usage on productivity levels in developing countries from 2003 to 2017. It reveals a notable positive correlation between increased use of pirated software and productivity, supported by various productivity indicators and control variables such as education, investment, and openness. These findings emphasize the need to address software piracy while also highlighting the potential role of education, investment, and openness in fostering productivity growth in developing nations.

The research paper extensively investigates privacy challenges in organizational data sharing, highlighting disparities in privacy policies and advocating for comprehensive technical guidance to address these obstacles effectively. By analyzing various data-sharing models, the paper exposes inherent privacy risks and emphasizes compliance with regulations like the GDPR. It underscores the critical role of robust industrial privacy frameworks in safeguarding sensitive data while enabling legitimate data-sharing efforts, offering practical insights and recommendations to enhance privacy management practices within organizations.

The paper extensively surveys deep learning techniques used in data hiding, specifically in digital watermarking and steganography, categorizing and comparing existing models across dimensions like network architecture, noise injection methods, and evaluation metrics. It emphasizes the intricate trade-offs between capacity, imperceptibility, and robustness in these methods and provides insights into their architectures, features, and limitations, aiding researchers and practitioners in selecting appropriate techniques.

The paper advocates for enhancing interconnection network security through the implementation of IPSec and Mac Address

Filtering authentication methods, given the evolving industry landscapes and heightened security threats. It details the components of IPSec, including Authentication Header (AH), Encapsulating Security Payload (ESP), and Internet Key Exchange (IKE), emphasizing their roles in ensuring data integrity, confidentiality, and authentication during transmission. Furthermore, the paper explores Quality of Service (QoS) analysis using tools like Wireshark to optimize network performance, providing a comprehensive overview of design and implementation methodologies for IPSec and Mac Address Filtering in interconnection networks.

The literature survey provides a comprehensive overview of diverse software security models and frameworks, spanning hierarchical models for quantifying software security, lightweight secure document retrieval, and social networking frameworks for requirements elicitation. It also explores security assessment frameworks for IoT services, operational security assurance evaluation of networked IT systems, and the importance assessment of security measures. Additionally, the survey delves into verifiable security protocols for smart healthcare, security analysis of IoT devices, and the impact of continuous software engineering practices, continuous integration, and software refactoring on quality attributes.

The literature survey delves deeply into advancements in cryptography, spanning topics such as secure communication protocols, symmetric and public key cryptography, post- quantum cryptography, homomorphic encryption, and blockchain technology. It examines key aspects like key management, secure multi-party computation, lightweight cryptography, zero-knowledge proofs, cryptographic hash functions, and attribute-based encryption, providing insights into their applications and future trajectories. These cryptographic innovations are pivotal in bolstering data security, safeguarding sensitive information, and fortifying secure communication channels within the digital realm.

The literature survey emphasizes the importance of user awareness and adoption of security measures in mobile security, combining review methods to explore threats, user behaviors, and countermeasures. Key findings reveal the prevalence of authentication methods like fingerprint scanners and PINs, underscoring the necessity for continuous updates and patching of mobile operating systems and applications. Additionally, the survey underscores the critical need for regular data backups and encryption to thwart data loss or unauthorized access, alongside highlighting the significant threat posed by social engineering techniques, emphasizing the urgency of educating users to recognize and evade such attacks.

This article delves into the design and analysis of self-protection and adaptive security for software-intensive systems, emphasizing the necessity of dynamic defense mechanisms against cyber-attacks. The research project focuses on enhancing the security of architecture-based self-adaptive systems by integrating self-protection capabilities, attack monitoring, and decentralized security measures. It explores diverse approaches, such as employing machine learning algorithms for threat detection and response, to effectively achieve adaptive security in software-intensive environments.

3. Proposed system:

The proposed system (Fig 1) represents a pinnacle of innovation and meticulous design, meticulously engineered to address the multifaceted challenges inherent in software licensing and protection within today's dynamic digital landscapes. It embodies a holistic approach that amalgamates cutting-edge technologies and advanced algorithms, aiming not only to fortify the security of software assets but also to provide users with a seamless and intuitive experience in managing their licenses. At its core, the utilization of PyQt6, a versatile Python framework renowned for its prowess in crafting intuitive graphical user interfaces (GUIs), underscores the system's commitment to user- centric design. By leveraging PyQt6, the system empowers users with a fluid and intuitive interaction experience, facilitating effortless navigation through its features and functionalities.

Central to the system's architecture is its seamless integration with the Google Drive API, a robust cloud-based storage and management platform offered by Google. This integration extends unparalleled convenience to users, enabling them to securely store, access, and manage their software licenses across a myriad of devices and platforms. Leveraging Google Drive's advanced infrastructure and stringent security measures, the system not only enhances data accessibility but also fortifies data security, instilling confidence in users regarding the safeguarding of their invaluable licensing information.

The bedrock of the system's security framework lies in its adept utilization of cryptographic techniques, serving as an impenetrable barrier against unauthorized access and data breaches. Through the employment of sophisticated algorithms such as the Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA), the system encrypts sensitive licensing data to render it indecipherable to unauthorized entities. Furthermore, the system adopts steganography, a sophisticated method for concealing information within digital media, to embed licensing data within seemingly innocuous image files. This clandestine integration fortifies the system's security posture, rendering it exceedingly challenging for malicious actors to intercept or extract sensitive data undetected.

In a proactive stride towards bolstering security, the system implements dynamic key generation and management protocols, ensuring the uniqueness and integrity of software installations. Each installation is endowed with a unique device identifier, such as a Media Access Control (MAC) address, which serves as a pivotal authentication key for validating the legitimacy of software licenses. This dynamic key generation process mitigates the risks associated with unauthorized duplication or distribution of software licenses, while robust key management protocols safeguard the confidentiality and integrity of generated keys, minimizing the likelihood of key compromise or misuse.

To fortify its defenses against piracy attempts, the system incorporates real-time monitoring and enforcement mechanisms, enabling swift detection and mitigation of suspicious activities. By continuously scrutinizing software usage patterns and license compliance, the system identifies anomalies and takes proactive enforcement actions, such as license revocation for unauthorized installations or the incapacitation of pirated copies. These proactive measures safeguard software assets and mitigate revenue loss stemming from unauthorized distribution and usage, reinforcing the system's stature as a stalwart guardian of software assets.

In summary, the proposed system epitomizes a comprehensive and sophisticated solution tailored to the intricate realm of software licensing and protection. By amalgamating advanced cryptographic algorithms, steganographic techniques, dynamic key management, and real- time monitoring capabilities, the system stands as a beacon of innovation, delivering unparalleled security features while prioritizing usability and accessibility for users in today's ever-evolving digital landscape. The DFD diagram of model (Fig. 2)

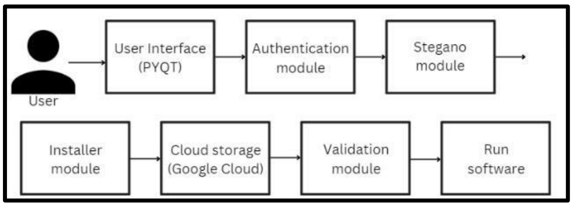


Figure. 1: Proposed System Architecture

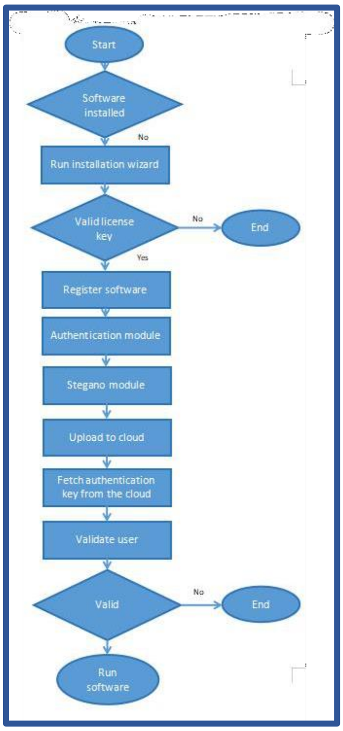
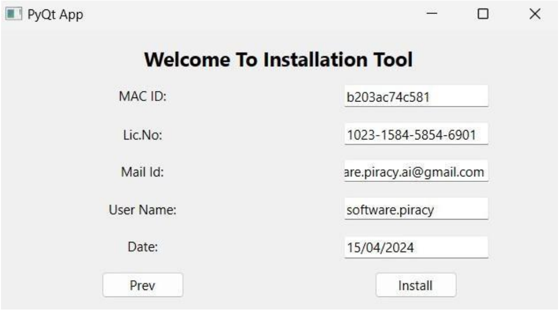


Figure. 2: Data Flow Diagram

4. Result:

The system underwent rigorous evaluation to assess its functionality, focusing on software license generation, data security, and compliance enforcement. Results highlighted its reliability in combatting software piracy, but also suggested areas for improvement. Key evaluations included license generation, which proved efficient and user- friendly, supported by cloud-based integration for seamless distribution. Security assessments confirmed robust encryption and steganography methods, with additional measures like MAC address verification enhancing security.

Performance evaluations revealed consistent performance and scalability, even under high loads, affirming the system's suitability for real-world deployment. Nonetheless, optimizations for faster license verification and broader software compatibility were identified as areas for improvement based on user feedback. The system effectively addresses software piracy, promoting legitimate usage through innovative technologies and security measures. While offering promising implications for productivity and digital security, ongoing research is necessary to refine features and tackle emerging challenges in software piracy and cyber security. The results are present in Fig. 3, 4 and 5.



Welcome To Installation Tool

MAC ID: b203ac74c581

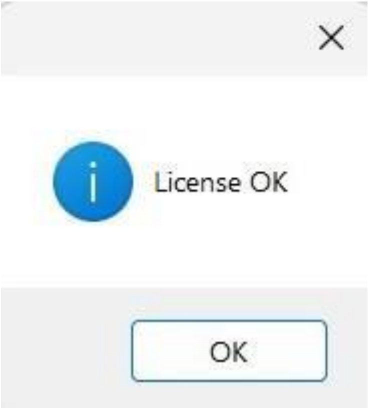
Lic.No: 1023-1584-5854-6901

Mail Id: are.piracy.ai@gmail.com

User Name: software.piracy

Date: 15/04/2024

Figure. 3: User details for installation



License OK

Figure. 4: License valid

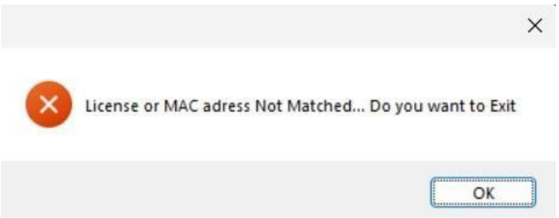

License or MAC adress Not Matched... Do you want to Exit

Figure. 5: Invalid License or MAC address

5. Conclusion:

In conclusion, the system presented in this paper offers a comprehensive solution for addressing software piracy and enhancing productivity in developing countries. By leveraging technologies such as PyQt6, Google Drive API, and steganography, the system facilitates secure software licensing and distribution while mitigating piracy risks. The findings underscore the significance of implementing measures to combat software piracy, as well as the potential of education, investment, and openness in fostering productivity growth. However, further research is warranted to explore the long-term implications of piracy on economic development and to refine the proposed system for broader applicability in the digital ecosystem.

6. References:

(1) Yalç?nkaya Koyuncu, J., & Ünver, M. (2023). Software Piracy and Productivity: Evidence from Developing Countries. Gümü?hane Üniversitesi Sosyal Bilimler Dergisi, 14(3), 889-897.

(2) Ghorashi, S. R., Zia, T., Bewong, M., & Jiang, Y. (2023). An Analytical Review of Industrial Privacy Frameworks and Regulations for Organisational Data Sharing. Applied Sciences, MDPI

(3) Wang, Z., Byrnes, O., Wang, H., Sun, R., Ma, C., Chen, H., Wu, Q., & Xue, M. (2023). Data Hiding with Deep Learning: A Survey - Unifying Digital Watermarking and Steganography. CSIRO's Data61, Australia, the University of Adelaide, Australia the University of Sydney, Australia, *the University of Queensland, Australia.

(4) Mochamad Akbar Fajar Hidayat Putra, Ucuk Darusalam, Andri Aningsih. (2020). Application of IP Security and Mac Address Filtering Authentication Methods to Build

Encrypted Interconnection Networks. *Jurnal Mantik, 4*(1), 343-353. E-ISSN 2685-4236.

(5) Korir, F. C. (2023). Software security models and frameworks: An overview and current trends. World Journal of Advanced Engineering Technology and Sciences, 08(02), 086-109.

(6) Victor, M., Praveenraj, D. D. W., Sasirekha, R., Alkhayyat, A., & Shakhzoda, A. (2023). Cryptography: Advances in Secure Communication and Data Protection. E3S Web of Conferences, 399, 07010.

(7) Weichbroth, P., & ?ysik, ?. (2020). Mobile Security: Threats and Best Practices. Mobile Information Systems, 2020, Article ID 8828078, 1- 15.

(8) Skandylas, C. S. L. U. S. (2021). Paper presented at the 15th European Conference on Software Architecture: Doctoral Symposium, September 13-17, 2021, Växjö, Sweden. CEUR Workshop Proceedings (CEUR-WS.org), ISSN 1613-0073.