International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 06 | June – 2025 DOI: 10.55041/ISJEM04162
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

Decoy Shield: Leveraging AI and Decoy Strategies for Enhanced Protection Against Data Exfiltration and Automated Cyberattacks

1st Mr. V. Udhayakumar, 2nd G.Susidaran

1Professor, Department of Computer Applications, Sri Manakula Vinayagar Engineering College (Autonomous), Puducherry 605008, India
udhayakumar.mca@smvec.ac.in
2Post Graduate student, Department of computer Applications, Sri Manakula Vinayagar Engineering College (Autonomous), Puducherry 605008, India
susidaran246@gmail.com

Abstract: Intellectual Property (IP) is a critical asset for organizations, containing valuable innovations and proprietary knowledge that must be protected to maintain a competitive edge. Cyberattacks on IP have become more prevalent, with adversaries using automated systems to exfiltration and classify large volumes of documents to extract sensitive information like trade secrets.However, traditional IP protection methods, such as encryption and firewalls, are often ineffective against these advanced, automated threats. This project introduces the DARD (Decoy Approaches for Robust Protection against IP Theft) system, designed to disrupt automated classification methods by employing misleading techniques. To detect adversarial behavior, the system uses a Variational Autoencoder (VAE) to identify anomalous patterns in access and activity logs.

This project introduces the DARD (Decoy Approaches for Robust Protection against IP Theft) system, a novel defense framework designed to proactively disrupt automated IP theft mechanisms by embedding deceptive and misleading information.

DARD focuses on confusing machine learning-based document classifiers and topic modeling algorithms, thereby reducing the efficacy of adversarial reconnaissance and data mining.Once adversaries are detected, the DARD system generates a modified document repository that manipulates document clustering and topic modeling outcomes, making it difficult for adversaries to identify topics of interest.

The system uses four manipulation operations—Basic Shuffle, Shuffle Increment, Shuffle Reduction, and Change Topic—which replace original keywords with decoy ones, creating misleading clusters.

The proposed approach incorporates techniques such as text preprocessing using Natural Language Processing (NLP), feature extraction with Term FrequencyInverse Document Frequency (TF-IDF), document clustering with K-Means, and topic modeling using Latent Dirichlet Allocation (LDA). These methods ensure that even when adversaries attempt to analyze the documents, the results will be deceptive. This system effectively protects against the initial phase of IP theft and provides secure access for legitimate users through a secure enclave-based architecture.

Objectives:

1. To detect adversarial behavior using Variational Autoencoder (VAE) for anomaly detection in access and activity logs.
2. To identify suspicious document access patterns and unauthorized high-volume data extraction attempts.
3. To disrupt automated document clustering and topic modeling used by adversaries for IP theft.
4. To implement decoy-based techniques such as Basic Shuffle, Shuffle Increment, Shuffle Reduction, and Change Topic to mislead adversaries.
5. To ensure legitimate users retain seamless access to original documents through a secure enclave- based architecture.

Keywords: Insurance IP Repository, End User, Adversary Model, Adversary Detection, Document Manipulation, Document Repository Modification, Alert Generator, Notification

1. Literature Review

Sun et al. (2021) proposed a machine learning-based method to detect deceptive decoy documents in targeted email attacks. Their approach integrated NLP techniques with classifiers such as SVM or Random Forests to identify semantic patterns indicating deception. Using a proprietary dataset of 200 Chinese-language documents, they achieved high accuracy (97.5%) with a low false positive rate (3.1%). The system is adaptable to various network points and offers automated, language-aware detection. However, its reliance on a specific language dataset may limit generalizability, and frequent retraining may be necessary due to evolving attack patterns.

Khan et al. (2023) introduced a security framework for protecting sensitive medical data in fog computing networks using decoy documents and user behavior profiling. When suspicious activity is detected, decoy files are served to confuse potential attackers. Although specific algorithms are not detailed, machine learning-based anomaly detection is implied. The framework excels in real- time breach detection and computational efficiency. Still, challenges remain in maintaining decoys at scale and accurately profiling users, especially when facing insider threats or experienced adversaries.

Taofeek et al. (2022) developed a Cognitive Deception Model (CDM) that generates syntactically and semantically realistic decoy documents using neural-based NLG techniques. Unlike traditional fake content, CDM creates coherent, believable documents that mimic genuine texts, effectively deceiving attackers and reducing data exfiltration. The model's strength lies in its realism and effectiveness in increasing attacker cognitive load. Nevertheless, training such models is computationally expensive, and ensuring scalability and adaptability to various domains can be complex.

Xiong et al. (2020) presented the Fake Equation Engine (FEE), a tool designed to generate realistic fake equations to deter intellectual property theft in technical documents. FEE uses optimization algorithms to balance mathematical accuracy with deception, while FEE–FAST offers a lightweight variant for quicker execution. The system effectively misleads human evaluators and supports scalability. However, the optimization process can be resource-intensive, and the method's focus on equations limits its applicability to broader content types.

Goldstein et al. (2021) addressed the threat of DNN model IP theft by proposing a lightweight model obfuscation method that alters model weights based on cryptographic keys. Without the correct key, the model degrades in accuracy while maintaining plausible output, making unauthorized use less effective. The solution supports secure model distribution and execution using PKI and memory encryption. Although efficient and hardware-compatible, its effectiveness depends on secure hardware infrastructure and careful key management.

Zhang et al. (2023) introduced GAIT, a game-theoretic framework that defends against IP theft through strategic fake content injection in documents. Using Stackelberg game modeling and NLP techniques, GAIT confuses attackers analyzing content at a granular level. It increases the attacker's workload and remains robust even against intelligent adversaries. Though highly effective, the method may raise computational and document management overhead and relies on accurate modeling of adversary behavior.

1. Research Methodology

The research methodology for this project centers around the development and implementation of the DARD (Decoy Approaches for Robust Protection against IP Theft) system, which is designed to proactively protect intellectual property from sophisticated, automated cyber threats. The DARD system employs a two-pronged approach: detecting adversarial behavior and misleading automated document analysis systems. To identify malicious activity, a Variational Autoencoder (VAE) is used to analyze access and activity logs, learning normal usage patterns and flagging deviations as potential threats. Once an adversary is detected, the system generates a modified document repository that aims to confuse and mislead machine learning-based classification and topic modeling algorithms.

This is achieved through four specific manipulation operations—Basic Shuffle, Shuffle Increment, Shuffle Reduction, and Change Topic—that strategically alter or replace keywords in documents to create deceptive clusters and obscure true topics. The methodology incorporates natural language processing (NLP) techniques for text preprocessing, including tokenization, stop-word removal, and lemmatization. It also uses Term Frequency–Inverse Document Frequency (TF-IDF) for feature extraction, K- Means for document clustering, and Latent Dirichlet Allocation (LDA) for topic modeling. These tools enable the system to mislead adversaries during the reconnaissance phase by producing content that appears legitimate but yields misleading analytical results. Additionally, the entire framework is supported by a secure enclave-based architecture that ensures legitimate users maintain secure and uninterrupted access to genuine IP documents, thereby enhancing both security and usability.

2. Current Scenario of Decoy Shield

In today's cybersecurity landscape, traditional defense mechanisms such as encryption, firewalls, and access control systems are no longer sufficient to counter increasingly sophisticated and automated cyberattacks targeting intellectual property (IP) and sensitive data. Attackers now utilize AI-powered tools to perform large- scale document classification and data mining, making it easier to exfiltrate valuable information from organizational repositories. In response to these evolving threats, advanced protection frameworks like **Decoy Shield** have emerged, leveraging artificial intelligence and strategic deception to proactively disrupt adversarial efforts.

The Decoy Shield system introduces decoy-based countermeasures that mislead and confuse automated reconnaissance by injecting deceptive content into document repositories. It employs techniques such as document manipulation, topic obfuscation, and behavioral analysis to hinder adversaries from accurately identifying and extracting critical information. AI models, including Variational Autoencoders (VAEs), are integrated to monitor user activity patterns and detect anomalies indicative of malicious behavior. Moreover, NLP techniques, TF-IDF for feature extraction, K-Means clustering, and LDA topic modeling are used to create misleading document structures, further complicating data extraction attempts. As organizations increasingly recognize the need for dynamic and intelligent defense strategies, systems like Decoy Shield represent a shift toward proactive, deception-driven security models that protect sensitive assets while maintaining usability for legitimate users.

3. Challenges in Decoy Shield

Despite its innovative approach, the Decoy Shield system faces several challenges in effectively implementing AI and decoy strategies for cybersecurity. One of the primary challenges is ensuring that the decoy documents are convincing and contextually realistic enough to deceive advanced machine learning-based classification and topic modeling tools used by adversaries. Generating misleading content without affecting legitimate access or raising suspicion requires a delicate balance between deception and authenticity.

Additionally, designing adaptive algorithms that can keep pace with evolving adversarial tactics poses a significant difficulty. Attackers may eventually learn to recognize patterns in decoy generation, thereby reducing the system's effectiveness over time.

The system's reliance on NLP, TF-IDF, clustering, and topic modeling also introduces challenges related to computational efficiency, scalability, and accuracy, especially when handling large-scale document repositories. Integrating behavioral anomaly detection through VAEs further complicates the architecture, as it requires continuous learning from diverse and dynamic user behaviors without generating false positives. Moreover, maintaining data integrity, user privacy, and operational transparency while embedding decoy mechanisms remains a complex task. Addressing these challenges is essential to ensure that Decoy Shield remains a robust and sustainable solution against modern, automated data exfiltration threats.

4. Existing System

The existing systems for Intellectual Property (IP) protection and cybersecurity primarily rely on conventional security measures such as encryption, firewalls, intrusion detection systems (IDS), and access control mechanisms. While these methods are effective in safeguarding data from unauthorized access to a certain extent, they fall short when dealing with sophisticated, automated cyberattacks that utilize artificial intelligence and machine learning to extract and classify sensitive information.

Traditional systems do not typically incorporate deception or obfuscation techniques, making them vulnerable to advanced reconnaissance tools used by attackers to identify and exfiltrate valuable IP.

Furthermore, existing document-based security solutions lack dynamic defenses capable of misleading or disrupting automated systems during the data-mining process. As a result, once an adversary bypasses the perimeter defenses, they can often easily analyze and extract meaningful information from internal documents. These limitations highlight the need for a more proactive and intelligent defense strategy, such as the Decoy Shield system, which introduces deception-based techniques to confuse and mislead automated attacks.

Several existing systems are currently employed to protect intellectual property (IP) and sensitive documents from data exfiltration and cyberattacks.

Traditional firewalls and intrusion detection systems (IDS) help monitor and filter network traffic to prevent unauthorized access.

Encryption mechanisms are widely used to protect data both at rest and in transit, ensuring that even if data is intercepted, it cannot be read without the decryption key. Digital Rights Management (DRM) technologies restrict how users can interact with documents, such as preventing printing, copying, or forwarding.

Access control systems, including Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), enforce strict user permission policies. Data Loss Prevention (DLP) tools help identify and block the unauthorized sharing of sensitive data outside the organization.

Honeypots and honeyfiles serve as decoys to detect and analyze malicious activity. Additionally, blockchain is being explored as a method to create tamper-proof records for tracking document access and ownership.

5. Proposed System

The proposed system, *Decoy Shield: Leveraging AI and Decoy Strategies for Enhanced Protection Against Data Exfiltration and Automated Cyberattacks*, introduces a novel, proactive approach to cybersecurity by integrating artificial intelligence with deception-based techniques. Unlike traditional defense mechanisms, this system employs decoy strategies to confuse and mislead adversarial machine learning algorithms used in automated document classification and topic modeling.

It uses a secure enclave-based architecture to differentiate between legitimate users and potential threats. Upon detecting suspicious behavior using a Variational Autoencoder (VAE), the system activates the decoy mechanism, generating manipulated versions of documents.

These documents are altered using operations such as Basic Shuffle, Shuffle Increment, Shuffle Reduction, and Change Topic to embed deceptive keywords, thereby distorting clustering and topic analysis.

Text preprocessing, TF-IDF-based feature extraction, K- Means clustering, and Latent Dirichlet Allocation (LDA) are used to ensure the decoys appear realistic while remaining misleading to unauthorized systems. This intelligent defense significantly reduces the chances of successful IP theft while maintaining usability for authenticated users.

International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 06 | June – 2025 DOI: 10.55041/ISJEM04162
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

6. Architectural Design

The architectural design of the *Decoy Shield* system is built on a layered, modular framework that integrates AI- based detection, deceptive document generation, and secure access control.

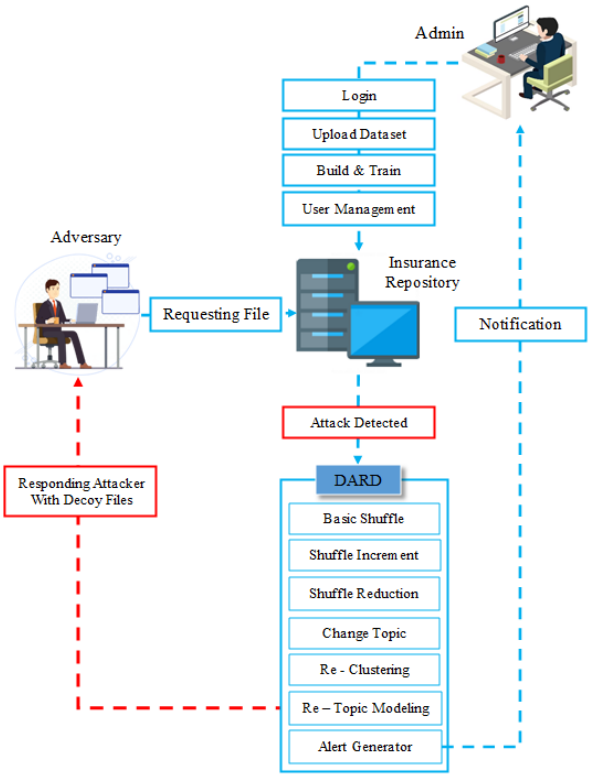

Fig. 1: Architecture Diagram

The architecture begins with a Monitoring and Logging Module, which continuously captures user access patterns and activity logs. These logs are then fed into a Detection Engine powered by a Variational Autoencoder (VAE), which identifies anomalies indicative of automated or adversarial behavior. Upon detecting such behavior, the system triggers the Decoy Generation Module, which modifies the original document repository using NLP- based techniques such as TF-IDF, K-Means clustering, and Latent Dirichlet Allocation (LDA). Four types of manipulation operations—Basic Shuffle, Shuffle Increment, Shuffle Reduction, and Change Topic—are applied to create deceptive but realistic-looking documents. A User Classification Layer ensures that only verified users can access the original documents, while suspicious entities are redirected to the manipulated dataset. This layered architecture enhances the system's robustness against IP theft by combining intelligent detection with proactive deception.

7. Modules

The Document-Based Question Answering System is composed of several key modules, each designed to ensure efficient document ingestion, question processing, answer generation, and user interaction. These modules work together to provide a seamless and intelligent question answering experience over user-uploaded documents. Insurance IP Repository

This module is the secure storage system for all intellectual property (IP) documents related to the insurance sector. It holds sensitive and proprietary documents, including policies, claims data, actuarial models, and research reports. The repository ensures data integrity and confidentiality through encryption and strict access controls, serving as the source of truth for document access requests.

1. End User

The End User module represents legitimate users such as employees, insurance agents, analysts, or partners who need access to the IP documents for their work. This module manages authentication and authorization to ensure only authorized personnel access sensitive information. It also facilitates seamless access to documents while maintaining secure and monitored interactions.

2. Adversary Model

This module defines the characteristics and behavioral patterns of potential attackers targeting the Insurance IP Repository. It models threats such as automated scraping, bulk downloading, and sophisticated classification attempts by adversaries. The adversary model informs detection strategies by outlining typical attack vectors and suspicious activity signatures.

3. Adversary Detection

Using advanced analytics and machine learning techniques (e.g., Variational Autoencoders), this module monitors access logs and user activities in real time to identify anomalies. It detects suspicious behaviors such as unusual query volumes, pattern deviations in document access, or rapid sequential downloads that may indicate automated IP theft attempts or cyberattacks.

4. Document Manipulation

Upon detecting adversarial activity, this module generates modified versions of documents by employing text manipulation techniques. It uses methods like keyword shuffling, topic alteration, and insertion of decoy information to confuse automated classification and topic modeling tools used by attackers. This helps in delivering misleading data to adversaries while safeguarding real IP.

5. Document Repository Modification

This module manages the creation and maintenance of a decoy document repository alongside the original. When an adversary is detected, the system redirects their access to this manipulated repository, ensuring they receive false or misleading content. Meanwhile, legitimate users continue to access the authentic repository without interruption. It handles synchronization, updates, and access controls between both repositories.

6. Alert Generator

This module automatically sends alerts to security teams when adversarial or suspicious activities are detected. Alerts contain relevant information such as user behavior patterns, accessed documents, and timestamps, enabling timely incident response and investigation.

7. Notification

The Notification module manages communication with

International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 06 | June – 2025 DOI: 10.55041/ISJEM04162
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

stakeholders, including end users and administrators. It delivers status updates, security warnings, and system messages through multiple channels such as email, SMS, or internal dashboards. Notifications also inform legitimate users of access anomalies or system changes to maintain transparency and trust.

8. Screenshots

Fig. 1: Home Page

Fig. 2: File Manipulation Page

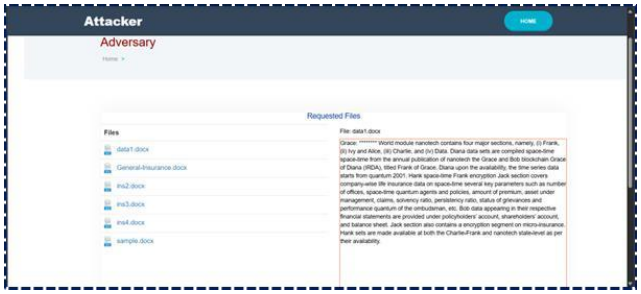

Fig. 3:Adversary finding Page

9. Key Features and Benefits of the Decoy Shield

The Document-Based Question Answering System is a sophisticated platform designed to simplify and accelerate information retrieval from a variety of document types. By integrating advanced technologies such as Optical Character Recognition (OCR), Natural Language Processing (NLP), and AI language models, the system delivers highly accurate and context-aware answers. This combination of features makes the system invaluable for users seeking efficient, precise, and versatile document querying capabilities.

1. Decoy Document Generation
   Creates manipulated versions of sensitive documents using keyword shuffling, topic alteration, and decoy data to mislead attackers.
2. Dual Repository Architecture
   Maintains both original and decoy IP repositories, allowing seamless access for legitimate users while feeding adversaries deceptive information.
3. Robust Access Control
   Ensures strict authentication and authorization for end users, minimizing the risk of insider threats and unauthorized access.
4. Automated Alerting System
   Provides instant notifications and alerts to security teams about suspicious activities, enabling quick response and mitigation.
5. Natural Language Processing Integration
   Employs NLP techniques for document preprocessing and feature extraction to improve the effectiveness of document manipulation and classification disruption.
6. Scalable and Secure Infrastructure
   Designed to handle large volumes of IP documents securely, with encryption and secure enclave-based access to safeguard data.

Benefits

1. Enhanced IP Protection
   Significantly reduces the risk of sensitive information theft by confusing automated classification and topic modeling tools used by attackers.
2. Early Threat Detection
   Detects adversarial behavior before significant data exfiltration occurs, minimizing potential damage.
3. Improved Competitive Advantage
   Protects proprietary knowledge and innovations, ensuring organizations maintain their market edge.
4. Minimized False Positives for Legitimate Users
   Allows authorized users uninterrupted and secure access to genuine documents while decoys target adversaries.
5. Cost-Effective Security
   Reduces reliance on traditional, reactive security measures by proactively disrupting data theft attempts.
6. Actionable Insights for Security Teams Delivers detailed alerts and behavioral insights, enhancing incident response and forensic investigations.

10. Opportunities Related to Decoy Shield

The **Decoy Shield** project presents significant opportunities in the evolving landscape of cybersecurity, particularly in the protection of intellectual property and sensitive data from sophisticated automated threats.

With the increasing reliance on AI-driven cyberattacks, there is a growing demand for intelligent and proactive defense systems like Decoy Shield.

This system leverages artificial intelligence and deceptive strategies to not only detect adversarial behavior but also to mislead and deter attackers, creating a powerful deterrent against data exfiltration.

Its ability to integrate with existing enterprise security infrastructures offers scalability and adaptability, opening opportunities for widespread adoption across sectors such as defense, healthcare, finance, and technology.

Furthermore, the system's modular design allows for continual improvement and customization based on industry-specific threats, presenting avenues for commercial development, research collaborations, and expansion into threat intelligence platforms.

As data breaches become increasingly costly and reputation-damaging, solutions like Decoy Shield provide a competitive advantage by enhancing organizational resilience and trust.

11. Conclusion

The *Decoy Shield* system represents a forward-thinking and robust solution to the growing threat of automated cyberattacks and intellectual property theft. By combining artificial intelligence with strategic deception techniques, the system not only detects malicious behavior but also proactively disrupts adversarial attempts to extract meaningful data. Through modules such as adversary detection, document manipulation, and alert generation, Decoy Shield ensures that sensitive information remains secure while misleading and disorienting attackers. The integration of techniques like NLP, TF-IDF, K-Means clustering, and LDA enhances the system's ability to manipulate document content and structure in a realistic yet deceptive manner. Ultimately, this innovative approach redefines data protection by moving beyond traditional perimeter defenses and offering dynamic, intelligent safeguards. As cyber threats continue to evolve, systems like Decoy Shield will be essential in maintaining the integrity, confidentiality, and competitive advantage of organizational data assets.

In the modern digital landscape, where data exfiltration and automated cyberattacks are increasingly sophisticated, the protection of intellectual property (IP) has become a critical concern for organizations across sectors. The *Decoy Shield* project addresses this challenge by introducing a novel, AI-driven, proactive defense mechanism that combines deception-based strategies with intelligent adversary detection.

Unlike traditional security measures—such as firewalls, encryption, or access control—that operate reactively or rely heavily on static defenses, Decoy Shield takes a dynamic and strategic approach. It confuses and misleads adversaries through the creation of deceptive document repositories, using Natural Language Processing (NLP), Term Frequency-Inverse Document Frequency (TF-IDF), K-Means clustering, and Latent Dirichlet Allocation (LDA) for realistic yet misleading content manipulation.

The system identifies anomalous patterns using a Variational Autoencoder (VAE) to detect adversarial activity early in the attack chain. Once detected, the system initiates operations such as keyword substitution, topic manipulation, and structural reshuffling to modify sensitive documents in a way that thwarts automated classification and topic inference tools commonly used by attackers.

Each module—from adversary detection to alert generation—works cohesively to ensure that the attacker is fed with false data, wasting their resources while legitimate users access only unaltered, verified documents within a secure enclave. Additionally, the alert system ensures real- time responses, enabling organizations to act swiftly when threats are detected.

Decoy Shield not only offers significant advantages in mitigating data theft but also introduces new opportunities in AI-powered cybersecurity research, adaptive deception modeling, and intelligent access control. Its flexible architecture makes it scalable and adaptable to a wide range of applications and organizational needs.

In summary, Decoy Shield transforms the way organizations defend their intellectual property by shifting from passive defense to active disruption. It redefines cybersecurity by leveraging intelligence, deception, and automation to stay ahead of cyber adversaries—offering a resilient and forward-looking solution in an era where information is both an asset and a target.

References

1. Andi Fariana and Syauqi Jinan, "The urgency of intellectual property rights in the digital era from the perspective of Sharia economic law in Indonesia", *Int. J. Res. Bus. Soc. Sci. (2147-4478)*, vol. 12, no. 8, pp. 552-556, 2023.
2. P. Kumar, "Intellectual Property Rights (IPR): Nurturing Creativity Fostering Innovation", vol. 02, no. 02, pp. 32-38, 2024.
3. F. Indra and F. Santiago, "Intellectual Property Rights in Legal Perspective in Indonesia", *Proc. First Multidiscip. Int. Conf.*, 2022.
4. X. Sun, X. Zhou, Q. Wang, P. Tang, E. L. C. Law and S. Cobb, "Understanding attitudes towards intellectual property from the perspective of design professionals", *Electron. Commer. Res.*, vol. 21, no. 2, pp. 521-543, 2021.

5. C. Tankard, “Advanced persistent threats and how to monitor and deter them,” Netw. Secur., vol. 2011, no. 8, pp. 16–19, Aug. 2011.
6. I. Ghafir and V. Prenosil, “Advanced persistent threat attack detection: An overview,” Int. J. Adv. Comput. Netw. Secur., vol. 4, no. 4, pp. 50–54, 2014.
7. Advanced Persistent Threat. Accessed: Apr. 6, 2021. [Online]. Available: https://en.wikipedia.org/wiki/Advanced_persistent_thr eat
8. W. Dai, M. Qiu, L. Qiu, L. Chen, and A. Wu, “Who moved my data? Privacy protection in smartphones,” IEEE Commun. Mag., vol. 55, no. 1, pp. 20–25, Jan. 2017.
9. Spear Phishing. Accessed: Apr. 6, 2021. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/spear-phishing
10. S. Le Blond, C. Gilbert, U. Upadhyay, M. G. Rodriguez, and D. Choffnes, “A broad view of the ecosystem of socially engineered exploit documents,” in Proc. Netw. Distrib. Syst. Secur. Symp., 2017, pp. 1–15.
11. irustotal: Free Online Virus, Malware and URL Scanner. Accessed: Apr. 6, 2021. [Online]. Available: https://www.virustotal.com
12. M. B. Salem and J. S. Stolfo, “Decoy document deployment for effective masquerade attack detection,” in Detection of Intrusions and Malware, and Vulnerability Assessment. Berlin, Germany : Springer, 2011, pp. 35–54.
13. M. B. Bowen, S. Hershkop, D. A. Keromytis, and J. S. Stolfo, “Baiting inside attackers using decoy documents,” in Security and Privacy in Communication Networks. Berlin, Germany : Springer, 2009, pp. 51–70.
14. J. Voris, N. Boggs, and S. J. Stolfo, “Lost in translation: Improving decoy documents via automated translation,” in Proc. IEEE Symp. Secur. Privacy Workshops, May 2012, pp. 129–133.
15. , J. Lee, and J. Hong, “How to make efficient decoy files for ransomware detection? ” in Proc. Int. Conf. Res. Adapt. Convergent Syst., 2017, pp. 208–212.
16. J. Voris, Y. Song, M. B. Salem, S. Hershkop, and S. Stolfo, “Active authentication using file system decoys and user behavior modeling: Results of a large scale study,” Comput. Secur., vol. 87, Nov. 2019, Art. no. 101412.
17. J. Lee, J. Choi, G. Lee, S.-W. Shim, and T. Kim, “PhantomFS: File-based deception technology for thwarting malicious users,” IEEE Access, vol. 8, pp. 32203–32214, 2020.
18. E. M. Rudd, R. Harang, and J. Saxe, “MEADE: Towards a malicious email attachment detection engine,” in Proc. IEEE Int. Symp. Technol. Homeland Secur. (HST), Oct. 2018, pp. 1–7.
19. R. Amin, J. Ryan, and J. van Dorp, “Detecting targeted malicious email,” IEEE Security Privacy Mag., vol. 10, no. 3, pp. 64–71, May 2012.
20. G. Ho, A. Sharma, M. Javed, V. Paxson, and A. D. Wagner, “Detecting credential spearphishing in enterprise settings,” in Proc. USENIX Secur. Symp., 2017, pp. 469–485.
21. J. Zhang, W. Li, L. Gong, Z. Gu, and J. Wu, “Targeted malicious email detection using hypervisor-based dynamic analysis and ensemble learning,” in Proc. IEEE Global Commun. Conf. (GLOBECOM), Dec. 2019, pp. 1–6.