XJTLU Entrepreneur College (Taicang) Cover Sheet

|  |  |  |
| --- | --- | --- |
| Module code and Title | **DTS306TC Security, Privacy and Ethics** | |
| School Title | **School of AI and Advanced Computing** | |
| Assignment Title | **Coursework 1** | |
| Submission Deadline | **5 pm China Time (UTC+8 Beijing) on Sat. 23nd Nov 2024** | |
| Final Word Count | **2000 +/-5%** | |
| If you agree to let the university use your work anonymously for teaching and learning purposes, please type **“yes”** here. | | **yes** |

I certify that I have read and understood the University’s Policy for dealing with Plagiarism, Collusion and the Fabrication of Data (available on Learning Mall Online). With reference to this policy I certify that:

* My work does not contain any instances of plagiarism and/or collusion. My work does not contain any fabricated data.

# By uploading my assignment onto Learning Mall Online, I formally declare that all of the above information is true to the best of my knowledge and belief.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Scoring – For Tutor Use** | | | | | | |
| **Student ID** | | | | 2143539  2036873  2144058  2141702  1927011 | | |
|  | | | | | | |
| **Stage of Marking** | | **Marker Code** | **Learning Outcomes Achieved （F/P/M/D）**  **(please modify as appropriate)** | | | **Final Score** |
| **A** | **B** | **C** |
| 1st Marker – red pen | |  |  |  |  |  |
| Moderation  – green pen | | **IM**  **Initials** | The original mark has been accepted by the moderator (please circle as appropriate): | | | Y / N |
|  | Data entry and score calculation have been checked by another tutor (please circle): | | | Y |
| 2nd Marker if needed – green  pen | |  |  |  |  |  |
| **For Academic Office Use** | | | **Possible Academic Infringement (please tick as appropriate)** | | | |
| **Date Received** | **Days late** | **Late Penalty** | * **Category A** | | Total Academic Infringement Penalty (A,B, C, D, E, Please modify where necessary) | |
|  |  |  | * **Category B** | |
| * **Category C** | |
| * **Category D** | |
| * **Category E** | |

**DTS306TC Coursework 1**

**Cyber Threats and Awareness in Finance Sector**

**Group10**

**Boyang.Li 2143539 [Boyang.Li21@student.xjtlu.edu.cn](mailto:Boyang.Li21@student.xjtlu.edu.cn)**

**Zheng.Zhou 2036873 [Zheng.Zhou20@student.xjtlu.edu.cn](mailto:Zheng.Zhou20@student.xjtlu.edu.cn)**

**Zi.Wang 1927011 [Zi.Wang19@student.xjtlu.edu.cn](mailto:Zi.Wang19@student.xjtlu.edu.cn)**

**Jinke.Li 2141702 [Jinke.Li21@student.xjtlu.edu.cn](mailto:Jinke.Li21@student.xjtlu.edu.cn)**

**Chengxi.Zhao 2144058 [Chengxi.Zhao21@student.xjtlu.edu.cn](mailto:Chengxi.Zhao21@student.xjtlu.edu.cn)**

# Contents

1. [Cyber Threats 3](#_bookmark2)
   1. [Background and Relevance 3](#_bookmark3)
2. [Cyber Threats Detection 4](#_bookmark7)
   1. [Email filtering and feature extraction 4](#_bookmark8)
   2. [Detection of Malicious Executables 4](#_bookmark9)
   3. [Intrusion Detection 5](#_bookmark10)
   4. [Anomaly Detection 5](#_bookmark10)
   5. [Ensemble Learning 5](#_bookmark10)
3. [Data Security, Privacy and Compliance 6](#_bookmark11)
   1. [The difference between data anonymization and encryption 6](#_bookmark12)
   2. [Challenges of data anonymization and pseudo-anonymization in digital finance 6](#_bookmark13)
   3. [Data Anonymization and GDPR Compliance 7](#_bookmark16)
4. [Future Digital Finance 8](#_bookmark20)
   1. [Policy Deficiencies 8](#_bookmark16)
   2. Recommended Improvements 9
   3. Dynamic Threat Response 9
   4. Ethical considerations 10

[References 1](#_bookmark21)0

[Member contribution 1](#_bookmark21)3

**Cyber Threats and Awareness in the Finance Sector**

**1. Cyber Threats**

In the digital age, the rapid development of technology has brought great benefits to the financial industry, streamlining transaction processes and improving customer experience. However, it has also opened new avenues for cyber threats, such as data theft and leakage, phishing, and ransomware. Cybercriminals exploit vulnerabilities in digital systems to gain unauthorized access, with disastrous consequences for institutions and individuals.

Among these threats, phishing is one of the most pervasive and dangerous cyber threats in digital finance. It involves attackers impersonating legitimate entities to deceive users into revealing sensitive information, such as login credentials and financial data. With the advancement of AI, phishing attacks have become more sophisticated and challenging to detect, posing a significant risk to data security and financial stability.

**1.1 Background and Relevance**

Phishing attacks exploit email systems, social media, and messaging platforms to deliver deceptive content. Financial institutions are particularly vulnerable, as phishing often targets high-value data [1] [3]. The integration of artificial intelligence exacerbates this threat:

Automated Email Generation: AI models, such as GPT, enable attackers to craft personalized phishing emails at scale [1].

Deepfake Technology: AI-generated audio and video deepfakes make impersonation more convincing [2].

Behavioral Analysis: Attackers leverage AI to analyze user behavior, tailoring phishing strategies to specific targets [3].

The implications of phishing include data breaches, financial losses, and reputational damage. For example, in 2020, a phishing attack on Twitter compromised high-profile accounts, causing both financial and trust-related repercussions [4].

Addressing these challenges requires integrating advanced detection technologies into existing cybersecurity frameworks.

**2. Cyber Threats Detection**

To effectively counter phishing attacks, we propose a sophisticated detection model that leverages state-of-the-art techniques. This multi-layered model integrates email filtering, malicious executable file detection, intrusion detection, anomaly detection, and ensemble learning to provide comprehensive and adaptive protection against evolving phishing tactics.

**2.1 Email filtering and feature extraction**

Phishing emails are the primary delivery mechanism for malicious content and fraudulent links. The first layer of the detection model uses machine learning algorithms based on natural language processing (NLP) to identify these emails. This approach involves extracting key features such as:

Email text and subject line: Advanced NLP techniques such as Word2Vec and BERT are used to analyze semantic relationships in the email body and subject line, allowing the model to understand intent and context [5].

Metadata: Sender email addresses, domain reputation, and attachment types are examined to identify suspicious patterns.

This layer of semantic understanding significantly reduces false positives because it can catch sophisticated phishing attempts designed to bypass simpler filters.

**2.2 Detection of Malicious Executables**

Phishing emails often contain malicious attachments, such as executables or scripts, designed to compromise the system when opened. Therefore, a binary classification system combining static and dynamic analysis forms the second layer of protection::

Static analysis: This approach examines file metadata, such as hashes, API call signatures, and DLL imports, to identify known malicious patterns. For example, identifying a hash match to a database of malware samples immediately flags the file [6].

Dynamic analysis: Files are executed in a sandbox environment where their runtime behavior is monitored. Unauthorized encryption attempts, command and control (C2) server communications, and unexpected API calls trigger alerts.

Deep learning integration: Convolutional neural networks (CNNs) enhance this layer by analyzing behavioral feature maps derived from dynamic analysis. These feature maps capture high-dimensional data, such as system call sequences, enabling the detection of obfuscated or new malware. CNNs excel at identifying non-linear patterns, which makes them particularly effective against zero-day threats. For

example, the CNN model can identify encrypted communications with suspicious IPs even if the malware employs advanced evasion techniques.

**2.3 Intrusion Detection**

Phishers often exploit vulnerabilities in networks to distribute malicious payloads or steal sensitive data. The third layer uses a real-time intrusion detection system (IDS)

to monitor network traffic and system logs. Key components include:

Feature extraction: Extract relevant features such as source IP address, destination port, traffic size, and protocol usage to characterize network behavior.

Detection model: Machine learning models such as recurrent neural networks (RNNs) and isolation forests analyze temporal patterns and deviations from normal traffic behavior [7].

Attention mechanism: By focusing on high-risk traffic patterns, the model minimizes false positives while ensuring that anomalies are detected in a timely manner.

This layer is critical for identifying complex attacks such as advanced persistent threats (APTs) that may involve subtle, long-term intrusions.

**2.4 Anomaly Detection**

User behavior monitoring is an important part of phishing detection because compromised accounts often exhibit unusual activity. The fourth layer uses unsupervised learning techniques to identify these anomalies:

Behavioral analysis: Autoencoders and clustering algorithms such as K-Means establish baselines for normal user behavior [8]. These include login time, geographic location, and transaction patterns.

Anomaly Algorithms: Behaviors that deviate from established patterns, such as sudden privilege escalation, excessive file downloads, or logins from multiple locations, are flagged for investigation.

For example, if a user account typically accesses files during office hours, but begins downloading large data sets from unfamiliar devices at night, the system will sound an alert. Multimodal analysis combines user behavior data with network activity logs, ensuring greater detection accuracy [8].

**2.5 Ensemble Learning**

The final layer integrates predictions from previous modules using "ensemble

learning techniques, such as random forests or voting mechanisms. This aggregation

enhances robustness and reduces the likelihood of false positives by combining evidence from multiple sources.

Robustness: Each detection layer provides unique insights, making the system resilient to single points of failure.

Adaptive Defense: As phishing tactics evolve, the ensemble approach enables the model to dynamically adapt, incorporating new detection patterns without compromising existing functionality.

By combining the results of email filtering, actionable analytics, intrusion detection, and anomaly monitoring, this layer provides a holistic assessment of potential threats [9].

**3. Data Security, Privacy and Compliance**

In the field of digital finance, it is particularly important to protect sensitive data from cyber threats. Data anonymization and encryption technology are currently important means to protect data privacy and meet compliance requirements. However, these two technologies have their own advantages and disadvantages in application, and the challenges they face also need to be explored and resolved in depth.

**3.1 The difference between data anonymization and encryption**

Data anonymization is to remove or blur personal identification information so that the data cannot be directly associated with a specific individual. For example, replace the customer's name with a unique identifier, or use differential privacy technology to prevent data leakage [10]. The main advantage of anonymization is that its data can be used for analysis and sharing, while reducing the risk of privacy leakage. However, the anonymized data cannot restore the original information.

Data encryption converts the original data into ciphertext through a specific algorithm, and only the user who holds the key can decrypt and access the original data. For example, the use of AES encryption technology to encrypt financial transaction information ensures that even if the data is intercepted, it cannot be read. The advantage of encryption is to protect the integrity and confidentiality of the data, but it consumes a lot of computing resources, and the decryption process may introduce potential risks [11].

**3.2 Challenges of data anonymization and pseudo-anonymization in digital finance**

In the field of digital finance, data anonymization and pseudo-anonymization face

the following main challenges:

**Data association attack:**

Even if the data is anonymized, attackers can still re-identify individuals by associating multiple data sets. For example, reconstructing user behavior patterns through

information such as transaction time and amount [12].

**Degradation of data quality:**

Anonymization may reduce the details of the data, affecting the ability of financial institutions to conduct accurate analysis and prediction [13].

**Technical complexity:**

Achieving efficient anonymization requires the combination of advanced algorithms (such as differential privacy), but the implementation cost of these technologies is

high [10].

**Legal compliance pressure:**

The standards for data anonymization vary in different countries and regions. For example, the EU's General Data Protection Regulation (GDPR) has strict requirements for anonymization and pseudo-anonymization [14].

**Solution:**

Use differential privacy technology to protect data privacy by adding random noise while maintaining data statistical characteristics [10].

Implement a dynamic data anonymization mechanism and adjust the degree of anonymization according to actual needs [10].

Strengthen the hierarchical management of financial data to ensure strict isolation of highly sensitive data from less sensitive data [11].

**3.3 Data Anonymization and GDPR Compliance**

The GDPR clearly stipulates that data controllers and processors must take reasonable measures to protect the privacy of personal data and implement data anonymization in certain circumstances [14]. Anonymization technology can help financial institutions meet GDPR compliance in the following aspects:

**Privacy protection:**

Through anonymization technology, financial institutions can strip personal identity information during data analysis, ensure that data is irreversibly desensitized, and reduce compliance risks [14].

**Data Sharing:**

Anonymized data can be safely used for third-party data sharing and cooperation without additional compliance review [13].

**Data Minimization Principle:**

The data minimization principle required by GDPR can be achieved through anonymization technology, that is, only non-sensitive desensitized data is used to

complete analysis tasks [14].

For example, a bank can use anonymization technology to ensure the privacy of customer data when conducting risk modeling without affecting the accuracy of the model. This approach not only meets GDPR requirements, but also enhances customer trust [13].

While addressing current challenges in data security and privacy, it is equally vital to

anticipate and prepare for future developments in digital finance, ensuring resilience against evolving cyber threats

**4. Future Digital Finance**

The digital financial landscape is evolving rapidly, but modern cyberattacks such as

advanced persistent threats (APTs) and ransomware have exposed significant shortcomings in current cybersecurity policies. These challenges highlight the urgent need for a robust, adaptable, and forward-looking approach to financial security in the face of increasingly sophisticated threats [15] [16].

**4.1 Policy Deficiencies**

One of the main challenges lies in the inconsistency of global cybersecurity standards. Financial institutions operating across jurisdictions must comply with conflicting regulations, such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States. This fragmentation creates compliance complexity, increases costs, and reduces operational efficiency [15].

Emerging technologies further exacerbate vulnerabilities. For example, smart contract vulnerabilities, such as the Poly Network hack in 2021 that resulted in losses of more than $600 million, reveal the inadequacy of current policies in addressing blockchain security risks. These vulnerabilities leave the financial system vulnerable to unauthorized access and manipulation of digital assets [17].

In addition, many organizations fail to effectively implement cybersecurity policies. The lack of regular audits, comprehensive risk assessments, and actionable assessment metrics undermines their ability to proactively identify and respond to potential threats. Policies are often reactive rather than preventative, leaving institutions ill-prepared for sophisticated attacks [15] [17].

**4.2 Recommended Improvements**

To address these shortcomings, a comprehensive, unified strategy is essential:

Unified Framework: A globally coordinated cybersecurity framework like Basel in the financial sector could harmonize standards and reduce regulatory complexity. Such a framework would establish clear guidelines for data protection, threat response, and compliance audits [15].

AI-driven compliance: Artificial intelligence (AI) can revolutionize compliance by automating the monitoring and coordination of regulations. AI tools can dynamically

analyze new and existing regulatory requirements, identify gaps, and generate

actionable recommendations to ensure alignment.

Ethical AI Integration: As financial institutions increasingly rely on AI for decision-making and security, ensuring transparency and fairness becomes critical. Policies must require clear documentation of AI models, establish accountability for decisions, and mitigate algorithmic biases that could disproportionately impact certain groups [16] [17].

**4.3 Dynamic Threat Response**

Cybersecurity must evolve alongside the threats it seeks to mitigate. AI plays a key

role in enhancing adaptability by:

Real-time monitoring: AI systems can dynamically detect and mitigate APTs by analyzing large amounts of data in real time to identify patterns that indicate malicious activity. This rapid response minimizes damage from complex, long-term attacks.

Reducing human risk: Employees remain a significant vulnerability in the financial system. Personalized cybersecurity training programs powered by AI can assess individual knowledge gaps and provide tailored educational content. This reduces the likelihood of human error, such as falling victim to phishing scams or social engineering attacks [15].

**4.4 Ethical considerations**

As digital finance becomes increasingly automated, ethical considerations must guide

the development and deployment of AI-driven systems. Ethical frameworks should:

Balance monitoring and privacy: Security measures must respect user privacy while

ensuring strong monitoring to detect threats.

Establish accountability for AI decisions: Institutions should clearly define responsibility for AI outcomes, especially in the case of errors or biases.

Enforce transparent practices: Financial institutions must adopt transparent processes for the use of AI so that stakeholders understand and trust these systems [17].

**5. Conclusion**

This report highlights the pervasive threat of phishing in digital finance, emphasizing the need for advanced detection mechanisms and robust data security practices. By integrating multi-layered detection systems, GDPR-compliant anonymization, and AI-driven policy improvements, financial institutions can enhance their resilience against cyber threats. A forward-looking approach combining technology, regulation, and ethical considerations will ensure the sustainable growth of digital finance in an evolving threat landscape.

**Reference**

1. Callsign, "How generative AI is driving a rise in phishing attacks," *Callsign*, [Online]. Available: [https://www.callsign.com/knowledge-insights/how-generative-ai-](https://www.callsign.com/knowledge-insights/how-generative-ai-is-driving-a-rise-in-phishing-attacks" \t "_new)

[is-driving-a-rise-in-phishing-attacks](https://www.callsign.com/knowledge-insights/how-generative-ai-is-driving-a-rise-in-phishing-attacks" \t "_new). [Accessed: Nov. 18, 2024].

[2] Help Net Security, "AI impersonation emerges as a potent cyberattack vector," *Help Net Security*, Oct. 24, 2024. [Online]. Available: [https://www.helpnetsecurity.com/2024/10/24/ai-impersonation-cyberattack-vector/](https://www.helpnetsecurity.com/2024/10/24/ai-impersonation-cyberattack-vector/" \t "_new). [Accessed: Nov. 18, 2024].

[3] F. F. Ali, R. Kumar, and J. Singh, "AI-driven phishing attacks and behavioral manipulation: Trends and implications," *Artificial Intelligence Review*, vol. 57, pp. 1-19, Oct. 2024. [Online]. Available: [https://link.springer.com/content/pdf/10.1007/s10462-024-10973-2.pdf](https://link.springer.com/content/pdf/10.1007/s10462-024-10973-2.pdf" \t "_new). [Accessed: Nov. 18, 2024].

[4] J. Barrett, "Twitter bitcoin scam: More than $100,000 stolen as accounts of Bill Gates, Elon Musk, Kanye West and others hacked," *Forbes*, Jul. 15, 2020. [Online]. Available: https://www.forbes.com/twitter-bitcoin-scam-2020. [Accessed: Nov. 2024].

[5] J. Devlin, M. W. Chang, K. Lee, and K. Toutanova, "BERT: Pre-training of deep bidirectional transformers for language understanding," *arXiv preprint arXiv:1810.04805*, Oct. 2018.

[6] J. Saxe and K. Berlin, "Deep neural network based malware detection using two dimensional binary program features," in *2015 10th International Conference on Malicious and Unwanted Software (MALWARE)*, Fajardo, PR, USA, 2015, pp. 11–20.

[7] R. Chalapathy and S. Chawla, "Deep learning for anomaly detection: A survey," *arXiv preprint arXiv:1901.03407*, Jan. 2019.

[8] C. C. Aggarwal and S. Sathe, "Theoretical foundations of outlier detection: A survey," in *Outlier Analysis*, 2nd ed., Cham, Switzerland: Springer, 2015, pp. 1–40.

[9] T. G. Dietterich, "Ensemble methods in machine learning," in *International Workshop on Multiple Classifier Systems*, Berlin, Germany, 2000, pp. 1–15.

[10] C. Dwork, "Differential privacy: A survey of results," in Proceedings of the 5th International Conference on Theory and Applications of Models of Computation (TAMC 2008), Xi'an, China, 2008, pp. 1-19.

1. K. K. R. Choo, "The cyber threat landscape: Challenges and future research

directions," Computers & Security, vol. 30, no. 8, pp. 719-731, Nov. 2011.

[12] A. Narayanan and V. Shmatikov, "Robust de-anonymization of large sparse datasets," in Proceedings of the 2008 IEEE Symposium on Security and Privacy (sp 2008), Oakland, CA, USA, 2008, pp. 111-125.

[13] A. Cavoukian and D. Castro, "Big data and innovation, setting the record straight: De-identification does work," Information and Privacy Commissioner of Ontario, Jun. 2014.

[14] European Parliament and Council of the European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)," Official Journal of the European Union, vol. L119, pp. 1-88, May 2016.

[15] S. H. Bhaharin, U. A. Mokhtar, R. Sulaiman, and M. M. Yusof, "Issues and Trends in Information Security Policy Compliance," in 2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS), Johor Bahru, Malaysia, 2019, pp. 1–6, doi: 10.1109/ICRIIS48246.2019.9073645.

[16] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security: Emerging trends and recent developments," Energy Reports, vol. 7, pp. 8176–8186, 2021, doi: 10.1016/j.egyr.2021.08.126.

[17] R. A. Alias, "Information security policy compliance: Systematic literature review," Procedia Computer Science, vol. 161, pp. 1216–1224, 2019, doi: 10.1016/j.procs.2019.11.230.

**Member contribution**

The following sections outline each team member’s specific contributions to the course and report:

Chengxi.Zhao(2144058):

Responsible for Part 1: Data Encryption in the coursework and Cyber Threats section of the report.

Excellently completed the task of encrypting the financial data in the fraud\_data.csv file using VeraCrypt software in Part 1. Contributed to the Cyber ​​Threat section of the report by analyzing various threats such as phishing, ransomware, and data theft, and providing relevant examples and background information.

Zi.Wang(1927011):

Contributed to the Cyber Threats Detection section of the report.

Developed the structure of this section, focusing on the latest technologies such as email filtering, intrusion detection, and anomaly detection. Proposed advanced solutions to mitigate cyber threats using machine learning and AI-based technologies.

Boyang.Li(2143539):

Responsible for the Data Security, Privacy, and Compliance section of the report.

Discussed the key differences between data anonymization and encryption, and highlighted challenges such as data correlation attacks and legal compliance. Proposed GDPR-compliant solutions to enhance data protection.

Jinke.Li(2141702):

Wrote the Future Digital Finance section of the report.

Explore policy gaps, emerging technology gaps, and the role of AI-driven compliance. Provide innovative recommendations to address dynamic threats and ethical considerations in digital finance.

Zhou.Zheng(2036873):

Responsible for Part 2 of the Coursework: Fraud Detection Model.

Excellently completed the code programming and model design required by the task, while assisting in overall report coordination to ensure the logical flow and coherence between different parts. Assisted in refining and proofreading the final report to ensure accuracy and completeness.