UNIVERSITY OF ST.GALLEN

School of Management, Economics,
Law, Social Sciences, International Affairs and Computer Science

---

Type of Paper

Title of Paper

Subtitle of Paper

Submitted by:
First name Last name
Matriculation number

Approved on Application by:

Professor:
Name and full title of professor

Date of Submission:

Day/Month/Year

Abstract

Lorem ipsum dolor sit amet, consectetur adipiscing elit.

Contents

List of Figures

List of Tables

List of Algorithms

Listings

1 Introduction

Recent cybersecurity literature has highlighted the paradigm shift in offensive and defensive strategies driven by the adoption of artificial intelligence, particularly the widespread availability of large language models (LLMs) This technological evolution has fundamentally altered the threat landscape, with both attackers and defenders leveraging AI capabilities to enhance their operations. The constantly evolving landscape of cybersecurity demands more sophisticated and adaptive defense strategies, as traditional static defense mechanisms prove increasingly insufficient against advanced persistent threats and zero-day vulnerabilities **gizzarelli2024**.

The integration of Artificial Intelligence (AI) and Machine Learning (ML) represents one of the most significant emerging trends in cybersecurity, revolutionizing threat detection and response by enabling systems to analyze vast amounts of data at unprecedented speeds, identify patterns, and predict potential threats before they materialize. Moreover, the advent of generative AI, a subset of AI focused on creating new content or data, presents both opportunities and challenges in the cybersecurity landscape, opening new possibilities for both attackers and defenders **gizzarelli2024**.

Honeypot technology has evolved similarly in response to these changes. AI-enhanced honeypots now offer improved credibility against sophisticated attackers **christli2024**, enhanced threat actor analysis capabilities through advanced behavioral monitoring **Otal2024**, and the ability to detect AI-powered attack vectors including autonomous LLM-based hacking agents **reworr2024**. Recent research has demonstrated that AI-driven honeypots powered by Large Language Models can dynamically generate contextually appropriate, human-like responses in real-time, greatly improving their ability to deceive and engage attackers **christli2024**.

However, while traditional honeypots suffer from limited interactivity and predictable behavior patterns that enable easy detection, existing research on AI-enhanced honeypots has yet to adequately address practical implementation frameworks, particularly for HTTP-based attack scenarios. The LLM in the Shell (SheLLM) project has shown promising results in creating generative honeypots for command-line interfaces **sladic2023**, but comprehensive frameworks for web-based protocols remain underexplored.

This research addresses the gap between theoretical AI honeypot concepts and production-ready systems by developing and evaluating a deployable AI/LLM-enhanced honeypot specifically designed for HTTP protocol interactions. The primary research question guiding this study is: How can large language models be effectively integrated into HTTP honeypots to create more convincing, interactive decoy systems while maintaining operational feasibility for production environments?

The related work section examines various approaches to AI honeypot implementations, including model training methodologies for cybersecurity applications **gizzarelli2024**, the integration of model-context protocols (MCP) in honeypot architectures, and threat mitigation strategies. Additionally, it explores containerized deployment approaches using Docker and analyzes how open-source developments in this field diverge from current academic research efforts.

The methodology section details the tools and frameworks employed in developing the honeypot system, establishing baseline requirements for cost-effectiveness, infrastructure needs, and performance expectations. Particular attention is given to the trade-offs between AI model sophistication and operational constraints, drawing insights from recent advances in test-time scaling for language models **muennighoff2025**.

The results section presents implementation challenges and key discoveries, while addressing critical ethical and technical considerations inherent in honeypot deployment. This includes discussion of legal compliance, data privacy concerns, and responsible disclosure practices, particularly important given the sophisticated deception capabilities of AI-enhanced systems **spitzner2003**.

The ability to quickly and accurately interpret data from security systems is paramount in the ever-evolving cybersecurity landscape. To enhance the effectiveness of honeypots, this research incorporates automatic mapping of collected logs to the MITRE ATT&CK framework, a comprehensive and widely recognized knowledge base of adversary tactics and techniques **gizzarelli2024**. By making this mapping process dynamic, security teams can immediately contextualize the activities observed in honeypot logs, identifying specific attack patterns and understanding the broader strategy behind intrusion attempts.

This thesis contributes to the field by implementing a production-ready AI/LLM honeypot for HTTP protocol interactions, capable of mimicking authentic web services, intelligently analyzing incoming requests, generating contextually appropriate responses, and maintaining response consistency through intelligent caching mechanisms. The convergence of AI-driven dynamic honeypots with automatic log mapping to frameworks like MITRE ATT&CK represents a new era of evolved cybersecurity, where complex systems can grow by integrating generative AI into honeypots, creating interactions that challenge even the most experienced attackers **gizzarelli2024**.

2 Literature Review

This section reviews key academical papers around the subject of AI/LLM-based Honeypots allowing a better understanding of the current field and its possible future developpement.

2.1 Traditional Honeypot Technologies and Limitations

Honeypots are computer systems designed to capture unauthorized activity by emulating operating systems, applications or services, serving as decoy systems whose primary function is to be attacked or compromised **spitzner2003**. The foundational work by Spitzner established honeypots as critical tools for catching insider threats and understanding attacker methodologies **spitzner2003**. They are broadly categorized by their level of interaction, which determines how well they emulate a target device and how easily an attacker can identify them as a honeypot **dodson2022**.

Low-interaction honeypots typically emulate only a limited set of services, providing minimal interaction while making them easy to set up and configure for gathering basic information about known attack patterns with reduced risk **Ng2021**. The comprehensive framework analysis by Ng et al. demonstrates that these systems excel in automated attack detection but struggle with sophisticated human-operated threats **Ng2021**. Examples include Honeyd, which allows users to create virtual hosts simulating various operating systems and services to observe scanning and unauthorized access attempts, representing one of the most widely deployed low-interaction solutions **Ng2021**.

In contrast, high-interaction honeypots mimic entire systems with real operating systems and services, providing extensive interaction capabilities to capture comprehensive data and discover new types of attacks and malware **Ng2021**. Industrial Control Systems (ICS) honeypot networks, as demonstrated by Dodson et al., showcase the effectiveness of high-interaction systems in detecting targeted attacks on critical infrastructure, revealing sophisticated attack patterns that would be missed by simpler solutions **dodson2022**. However, these systems are notably more complex to deploy and manage, requiring careful planning for monitoring, logging, firewalls, and intrusion detection systems to prevent attacker escape into production environments **dodson2022**.

Adaptive honeypot configuration strategies have emerged as a response to traditional limitations, with Fraunholz et al. proposing dynamic deployment and maintenance approaches that can adjust to evolving threat landscapes **frauenholz2017**. Their research demonstrates that adaptive configurations can significantly improve detection rates while reducing maintenance overhead compared to static deployments **frauenholz2017**.

Performance analysis of traditional honeypot systems has demonstrated both their effectiveness and limitations in real-world deployments. Fuzi's comprehensive analysis of T-Pot honeypots revealed significant capabilities in network intrusion detection, providing valuable insights into attack patterns and threat behaviors while highlighting the challenges of processing large volumes of honeypot data **fuzi2024**. The study showed that traditional honeypots excel at capturing automated attacks but struggle with sophisticated, human-operated campaigns that can adapt their behavior based on system responses **fuzi2024**.

The taxonomy for dynamic honeypot measures of effectiveness established by Pittman et al. provides a structured framework for evaluating honeypot performance, identifying key limitations in traditional approaches **pittman2020taxonomy**. Their research reveals that static honeypots lack the ability to adapt to evolving attack patterns and may become obsolete as attackers develop new techniques for honeypot detection **pittman2020taxonomy**. Limited interaction capabilities in low-interaction systems consistently fail to capture sophisticated multi-stage attacks that require deeper system engagement and sustained attacker interaction.

Detection by experienced attackers remains a significant concern, as traditional honeypots often exhibit predictable behavior patterns that can reveal their deceptive nature to skilled adversaries. The scalability challenges of high-interaction honeypots make them resource-intensive to deploy and maintain across large networks, while manual configuration and maintenance requirements create operational overhead that limits their practical deployment in many organizations **pittman2020taxonomy**. These fundamental limitations have driven the cybersecurity community toward developing more sophisticated, AI-enhanced honeypot systems that can address many of these traditional shortcomings through adaptive behavior and intelligent response generation.

2.2 AI and Machine Learning in Cybersecurity

The integration of Artificial Intelligence (AI) and Machine Learning (ML) has revolutionized cybersecurity by enabling systems to analyze vast amounts of data at unprecedented speeds, identify patterns, and predict potential threats before they materialize **gizzarelli2024**. AI-driven tools can automatically detect anomalies, reduce false positives, and prioritize the most critical threats, thereby enhancing the efficiency and effectiveness of cybersecurity efforts.

Machine learning applications in threat detection and analysis have demonstrated significant improvements over traditional signature-based approaches. Supervised learning algorithms trained on labeled datasets can identify known attack patterns with high accuracy, while unsupervised learning techniques excel at detecting previously unknown threats by identifying deviations from normal behavior patterns. Deep learning models, particularly neural networks, have shown remarkable success in analyzing complex data structures such as network traffic, system logs, and malware binaries.

Behavioral analysis using ML techniques has emerged as a particularly powerful approach for identifying sophisticated attacks that evade traditional detection methods. These systems analyze user behavior, network patterns, and system activities to establish baseline behaviors and detect anomalous activities that may indicate compromise. Machine learning models can adapt to new attack patterns by continuously

learning from observed behaviors, making them more resilient against evolving threats.

Adversarial AI in cybersecurity contexts presents both opportunities and challenges. While AI systems can be used to enhance defensive capabilities, they can also be exploited by attackers to develop more sophisticated attack methods. AI-powered attack generation techniques can create adaptive malware, generate convincing phishing content, and automate reconnaissance activities. This arms race between AI-enhanced attacks and defenses necessitates continuous advancement in defensive AI technologies.

The application of AI in cybersecurity extends to automated incident response, where machine learning algorithms can analyze security events, correlate threat indicators, and recommend or automatically execute response actions. Natural Language Processing (NLP) techniques enable the automated analysis of threat intelligence reports, extracting relevant indicators of compromise (IoCs) and mapping them to established threat frameworks such as MITRE ATT&CK.

2.3 AI-Enhanced Honeypot Systems

The convergence of artificial intelligence and honeypot technology represents a significant advancement in cybersecurity defense strategies. Early AI honeypot implementations focused primarily on automated response generation and basic behavioral adaptation. However, recent developments have leveraged advanced machine learning techniques, particularly large language models (LLMs), to create more sophisticated and convincing deception environments.

Machine learning for honeypot data analysis has transformed how organizations process and interpret the vast amounts of data collected by honeypot systems. Traditional honeypots generate extensive logs that require manual analysis to extract meaningful insights. AI-enhanced systems can automatically analyze this data, identify attack patterns, classify threats, and generate actionable intelligence for security teams.

Dynamic honeypot adaptation using AI enables systems to modify their behavior in real-time based on attacker actions and emerging threat patterns. These adaptive systems can change their apparent vulnerabilities, modify response patterns, and even alter their simulated operating environment to maintain attacker engagement and gather more comprehensive intelligence **Otal2024**.

Comparison of different AI approaches reveals distinct advantages and limitations. Rule-based systems offer predictable behavior and easier debugging but lack the flexibility to handle novel attack scenarios. Machine learning approaches provide better adaptability and can learn from new attack patterns but may require extensive training data and can be more difficult to interpret. Deep learning models, particularly transformer-based architectures, offer the most sophisticated response generation capabilities but require significant computational resources.

Recent research has demonstrated the effectiveness of LLM-powered honeypots in creating convincing interactive environments. The SheLLM project represents a pioneering effort in this field, leveraging large language models to simulate realistic command-line interfaces that can engage attackers in extended interactions while maintaining believable system behaviors **sladic2023**. These systems can generate contextually appropriate responses to complex commands, maintain session state across multiple inter-

actions, and adapt their behavior based on attacker actions.

Advanced LLM honeypot implementations have shown significant improvements in attacker engagement and intelligence gathering capabilities **Otal2024**; **reworr2024**. These systems demonstrate the potential for large language models to create sophisticated interactive deception environments that can maintain prolonged attacker engagement while collecting comprehensive behavioral data.

The integration of generative AI technologies has enabled honeypots to simulate various operating systems, applications, and services with unprecedented realism. These systems can generate dynamic content, respond to novel queries, and maintain consistent personalities across extended engagements. The ability to process natural language inputs and generate human-like responses makes AI-enhanced honeypots particularly effective against social engineering attacks and human-operated threats **christli2024**.

2.4 Model Training for Cybersecurity Applications

Training data requirements and datasets for security models present unique challenges in the cybersecurity domain. Unlike many other machine learning applications, cybersecurity models require datasets that accurately represent real-world attack patterns while maintaining ethical and legal boundaries. The sensitive nature of cybersecurity data often limits the availability of comprehensive training datasets, necessitating innovative approaches to data collection and sharing.

Domain-specific model fine-tuning approaches have emerged as essential techniques for adapting general-purpose AI models to cybersecurity applications. Pre-trained language models can be fine-tuned on cybersecurity-specific datasets to improve their understanding of technical terminology, attack methodologies, and appropriate response patterns. This approach leverages the broad knowledge encoded in large-scale pre-trained models while specializing them for cybersecurity tasks.

Transfer learning in cybersecurity contexts enables the application of knowledge gained from one security domain to another. Models trained on network intrusion data can be adapted for malware analysis, and techniques developed for one type of honeypot can be transferred to different deployment scenarios. This approach is particularly valuable given the limited availability of labeled cybersecurity datasets.

Model training for deception and social engineering scenarios requires careful consideration of ethical implications and potential misuse. Training data must include realistic but appropriately sanitized examples of social engineering attacks, phishing attempts, and other human-targeted threats. The challenge lies in creating models that can effectively simulate these interactions for defensive purposes without enabling malicious applications.

Evaluation metrics for security-focused AI models must account for the unique requirements of cybersecurity applications. Traditional machine learning metrics such as accuracy and precision remain important, but security-specific metrics such as false positive rates, detection time, and attacker engagement duration become critical measures of effectiveness. The development of standardized evaluation frameworks for AI-enhanced cybersecurity systems remains an active area of research.

Challenges in creating realistic training datasets include the need to balance realism with privacy and

security concerns. Synthetic data generation techniques offer promising solutions by creating artificial datasets that maintain the statistical properties of real cybersecurity data without exposing sensitive information. Advanced generative models can create realistic network traffic patterns, system logs, and attack scenarios for training purposes.

Few-shot and zero-shot learning applications are particularly relevant in cybersecurity, where new attack patterns emerge continuously. These techniques enable AI models to adapt to new threats with minimal training data, leveraging their existing knowledge to understand and respond to novel attack scenarios. This capability is crucial for maintaining effectiveness against rapidly evolving cyber threats **muennighoff2025**.

Model training innovations such as simple test-time scaling have shown promise in improving the performance of AI models in complex reasoning tasks, which has direct applications in cybersecurity scenarios where models must analyze and respond to sophisticated attack patterns in real-time **muennighoff2025**.

2.5 HTTP Protocol Security and Web-Based Attacks

Common HTTP-based attack vectors continue to represent a significant portion of cybersecurity threats, making web-focused honeypots essential components of modern defense strategies. Cross-site scripting (XSS), SQL injection, cross-site request forgery (CSRF), and various injection attacks exploit vulnerabilities in web applications and services. Understanding these attack patterns is crucial for developing effective honeypot systems that can attract and analyze web-based threats.

Web application security challenges stem from the complexity of modern web technologies and the diverse attack surface they present. The interaction between client-side and server-side components, the use of multiple programming languages and frameworks, and the integration of third-party services create numerous potential vulnerabilities. Honeypots designed to simulate these complex environments must accurately replicate these vulnerabilities while maintaining security boundaries.

HTTP honeypot implementations require careful consideration of protocol compliance and realistic behavior simulation. These systems must handle various HTTP methods, status codes, headers, and content types while maintaining believable responses to both legitimate and malicious requests. The challenge lies in creating systems that appear vulnerable to automated scanners while providing meaningful interaction for human attackers.

API security and monitoring represent increasingly important aspects of web-based cybersecurity. Modern applications rely heavily on REST APIs, GraphQL endpoints, and other web services that present unique attack vectors. Honeypot systems must simulate these interfaces convincingly, handling authentication mechanisms, parameter validation, and response formatting while collecting intelligence about API-focused attacks.

The integration of AI technologies into web-based honeypots enables more sophisticated simulation of web application behaviors. Machine learning models can generate dynamic content, simulate database interactions, and respond to complex query patterns. Natural language processing capabilities allow these

systems to handle text-based inputs in forms, comments, and user-generated content areas, providing more realistic interaction surfaces for attackers.

2.6 Containerization and Deployment Frameworks

Docker in cybersecurity applications has revolutionized the deployment and management of security tools, including honeypot systems. Containerization provides isolation, scalability, and reproducibility benefits that are particularly valuable for honeypot deployments. Docker containers can encapsulate entire honeypot environments, making them easily deployable across different infrastructure platforms while maintaining consistent behavior.

Container security considerations are crucial when deploying honeypot systems, as the goal of attracting attackers creates unique security challenges. Proper container isolation, resource limitations, and network segmentation become critical for preventing attackers from escaping the honeypot environment and accessing production systems. Security best practices for containerized honeypots include minimal base images, read-only file systems where possible, and comprehensive monitoring of container activities.

Scalable honeypot deployments benefit significantly from containerization technologies. Container orchestration platforms such as Kubernetes enable the automated deployment, scaling, and management of honeypot systems across large infrastructure environments. These platforms can dynamically create and destroy honeypot instances based on demand, distribute them across multiple nodes, and provide centralized logging and monitoring capabilities.

Cloud-based honeypot architectures leverage the scalability and flexibility of cloud computing platforms to create distributed honeypot networks. These deployments can span multiple geographic regions, simulate various infrastructure configurations, and scale automatically based on attack patterns and resource requirements. Cloud-native technologies such as serverless computing and managed services can reduce operational overhead while improving scalability.

The integration of AI technologies with containerized honeypot deployments enables sophisticated orchestration and management capabilities. Machine learning algorithms can analyze attack patterns and automatically adjust honeypot configurations, spin up additional instances in response to increased attack activity, and optimize resource allocation based on threat intelligence. Container platforms provide the infrastructure foundation for these AI-driven capabilities.

2.7 Threat Intelligence and Analysis

Automated threat intelligence gathering has become essential for maintaining situational awareness in the rapidly evolving cybersecurity landscape. AI-enhanced systems can continuously monitor threat feeds, analyze security reports, and extract relevant indicators of compromise (IoCs) from various sources. Natural language processing techniques enable the automated analysis of unstructured threat intelligence reports, converting human-readable descriptions into machine-processable data structures.

Threat actor profiling and attribution represent complex analytical challenges that benefit significantly

from machine learning approaches. AI systems can analyze attack patterns, tool usage, infrastructure preferences, and tactical approaches to identify similarities between different campaigns and potentially attribute them to specific threat actors or groups. This analysis relies on comprehensive datasets of historical attack data and sophisticated pattern recognition algorithms.

IoC (Indicators of Compromise) extraction from unstructured sources requires advanced natural language processing capabilities. AI systems must identify IP addresses, domain names, file hashes, registry keys, and other technical indicators within free-text reports while understanding their context and relevance. Machine learning models trained on cybersecurity datasets can achieve high accuracy in extracting and classifying these indicators.

Real-time threat analysis frameworks integrate multiple data sources, including honeypot logs, network telemetry, endpoint data, and external threat intelligence, to provide comprehensive threat assessment capabilities. AI algorithms can correlate events across these diverse data sources, identify complex attack patterns, and prioritize threats based on their potential impact and likelihood of success.

The application of honeypot data to threat intelligence analysis provides unique insights into attacker behavior and tactics. Unlike other security data sources that may only capture successful attacks or detection events, honeypots provide detailed logs of attacker interactions, tool usage, and tactical approaches. This data is particularly valuable for understanding the human element of cyber attacks and developing behavioral models of threat actors.

2.8 MITRE ATT&CK Framework

The MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework represents one of the most comprehensive and widely adopted approaches to understanding and categorizing cyber adversary behavior. Developed by the MITRE Corporation, this globally accessible knowledge base provides a structured approach to documenting adversary tactics and techniques based on real-world observations **gizzarelli2024**.

The framework organizes adversary behavior into a matrix structure that maps tactics (the ”why” of attacks) to techniques (the ”how” of attacks). This organization provides security professionals with a common language for discussing and analyzing cyber threats, facilitating improved communication and collaboration across the cybersecurity community. The framework encompasses multiple technology domains, including Enterprise, Mobile, and Industrial Control Systems (ICS), each representing different operational environments where adversaries operate.

The MITRE ATT&CK framework describes adversarial TTPs (Tactics, Techniques, and Procedures) using a structure of four increasingly granular levels: tactics, techniques, sub-techniques, and procedures. Tactics represent the high-level goals or objectives of adversaries, such as gaining credential access or establishing persistence. Techniques describe the specific methods used to achieve tactical objectives, while sub-techniques provide additional granularity for complex techniques that can be implemented in multiple ways.

Automatic mapping of cyber threat intelligence to the MITRE ATT&CK framework addresses one of the most significant challenges in applying this framework at scale. Traditional manual mapping processes are time-consuming and error-prone, particularly when dealing with large volumes of unstructured threat intelligence data. AI-powered mapping systems leverage natural language processing and machine learning techniques to automatically analyze threat reports and map relevant behaviors to appropriate ATT&CK techniques.

The integration of honeypot data with MITRE ATT&CK mapping provides unprecedented insights into attacker behavior and tactics. Systems like SYNAPSE-to-MITRE demonstrate the potential for real-time mapping of honeypot interactions to the ATT&CK framework, enabling security teams to understand attack patterns in the context of established threat models. This integration facilitates rapid threat assessment, incident response planning, and defensive strategy development.

Machine learning models for ATT&CK mapping face unique challenges related to the complexity and ambiguity of natural language descriptions of cyber threats. The SYNAPSE-to-MITRE extension addresses these challenges by training multilayer perceptron classifiers on curated datasets of cyber threat intelligence reports. The system's ability to provide multiple potential mappings for each analyzed sentence acknowledges the inherent ambiguity in threat descriptions while providing security analysts with comprehensive classification options.

2.9 Ethical and Legal Considerations

Legal frameworks for honeypot deployment vary significantly across jurisdictions and present complex challenges for organizations implementing deception technologies. The intentional creation of vulnerable systems designed to attract attackers raises questions about legal liability, data protection compliance, and the appropriate scope of defensive activities. Organizations must carefully consider applicable laws regarding computer fraud, unauthorized access, and data privacy when deploying honeypot systems.

Ethical guidelines for deception technologies require balancing the legitimate security benefits of honeypots against potential risks and unintended consequences. The use of deception in cybersecurity contexts raises questions about proportionality, necessity, and the potential for misuse. Professional organizations and industry groups have developed guidelines for the ethical deployment of honeypots, emphasizing the importance of proper authorization, scope limitation, and responsible data handling.

Privacy concerns and data protection represent significant considerations for honeypot deployments, particularly in jurisdictions with strict data protection regulations such as the European Union's General Data Protection Regulation (GDPR). Honeypots may collect personal information from attackers, including IP addresses, user agents, and potentially personally identifiable information entered during attacks. Organizations must implement appropriate privacy safeguards and ensure compliance with applicable data protection requirements.

Responsible disclosure practices become particularly important when honeypots discover new vulnerabilities or attack techniques. Organizations must balance the need to protect their own systems and share threat intelligence with the cybersecurity community against the potential risks of disclosing sensitive in-

formation. Established frameworks for responsible disclosure provide guidance for handling discoveries made through honeypot deployments.

The deployment of AI-enhanced honeypots introduces additional ethical considerations related to the use of artificial intelligence in security contexts. The potential for AI systems to engage in sophisticated deception raises questions about the appropriate limits of automated defensive activities. Organizations must consider the implications of using AI technologies that can learn from and adapt to attacker behavior, potentially leading to increasingly sophisticated deception capabilities.

Recent research on LLM agent honeypots has highlighted the importance of monitoring AI hacking agents in the wild, providing insights into how malicious actors might leverage AI technologies for offensive purposes **reworr2024**. This research underscores the need for ethical guidelines that address the dual-use nature of AI technologies in cybersecurity contexts.

International cooperation and information sharing through honeypot networks require careful consideration of legal and regulatory frameworks across multiple jurisdictions. The global nature of cyber threats necessitates international collaboration, but differences in legal systems, data protection requirements, and law enforcement approaches can complicate information sharing arrangements. Organizations participating in honeypot networks must navigate these complex legal landscapes while maintaining effective threat intelligence sharing capabilities.

A Appendix

This section contains additional material that supports the thesis, such as code listings, large data sets, or additional explanations.

A.1 Declaration of Authorship

The following text is to be attached to the thesis.

"I hereby declare,

- that I have written this thesis independently,
- that I have written the thesis using only the aids specified in the index;
- that all parts of the thesis produced with the help of aids have been declared;
- that I have handled both input and output responsibly when using AI. I confirm that I have therefore only read in public data or data released with consent and that I have checked, declared and comprehensibly referenced all results and/or other forms of AI assistance in the required form and that I am aware that I am responsible if incorrect content, violations of data protection law, copyright law or scientific misconduct (e.g. plagiarism) have also occurred unintentionally;
- that I have mentioned all sources used and cited them correctly according to established academic citation rules;
- that I have acquired all immaterial rights to any materials I may have used, such as images or graphics, or that these materials were created by me;
- that the topic, the thesis or parts of it have not already been the object of any work or examination of another course, unless this has been expressly agreed with the faculty member in advance and is stated as such in the thesis;
- that I am aware of the legal provisions regarding the publication and dissemination of parts or the entire thesis and that I comply with them accordingly;
- that I am aware that my thesis can be electronically checked for plagiarism and for third-party authorship of human or technical origin and that I hereby grant the University of St.Gallen the copyright according to the Examination Regulations as far as it is necessary for the administrative actions;
- that I am aware that the University will prosecute a violation of this Declaration of Authorship and that disciplinary as well as criminal consequences may result, which may lead to expulsion from the University or to the withdrawal of my title."

By submitting this thesis, I confirm through my conclusive action that I am submitting the Declaration of Authorship, that I have read and understood it, and that it is true.

Date and signature

……

A.2 Declaration of Confidentiality

Declaration of Confidentiality

in connection with written work at the University of St.Gallen

The following text has to be added to the work and signed:

The undersigned

hereby undertakes and warrants to treat any information obtained by the enterprise/ administration concerned in strict confidentiality. In particular, he / she shall only permit people other than the referees to inspect his / her written work with the express consent of all the parties that have provided information.

The undersigned hereby takes cognizance of the fact that the University of St.Gallen may check his / her work for any plagiarism with the help of a plagiarism software and that the undersigned shall have to notify the enterprise/administration surveyed accordingly.

Date and signature

……