

ciberai

by Laetitia Badaro

Submission date: 25-Apr-2024 10:33AM (UTC+0100)

Submission ID: 230760220

File name: 53435_Laetitia_Badaro_ciberai_568140_1047421962.docx (4.43M)

Word count: 2195

Character count: 12962

LEVEL 5 ASSESSMENT SPECIFICATION

Student name:	Laetitia badaro	Student ID number:	2325368
Programme:			
Module:	Changemakers: Creativity and Value Creation		
Module code:	ACCA5033	Contribution to Overall Module Assessment (%):	50%
Lecturer:	James MG Williams	Internal Verifier:	Divya Chidambaram
Assignment Title:	Assignment 2: Project Management & Innovation.	Word count (or equivalent):	2500 equivalent.
Submission deadline:	Thursday 25th April 2024.	Return date of provisional marks & written feedback:	Aim: Within 4 working weeks.
Submission method:	All written assessments, where practical and possible, must be submitted via Turnitin unless otherwise instructed by the Lecturer. (Please DO NOT put this assessment specification into Turnitin or it will match many similarities with other students' submissions.) Alternative submission method (if applicable): Late submission of the assessment will result in a late penalty mark. Penalties for late submission: Up to one week late, maximum mark of 40%. Over one week late, 0%. Only the Extenuating Circumstances Panel may approve a change to submission dates.		
Academic honesty / referencing:	Academic honesty is required. In the main body of your submission you must give credit to authors on whose research and ideas your work is based. Append to your submission a reference list that indicates the books, articles, etc. that you have used, cited or quoted in order to complete this assessment.		

**Module Learning Outcomes
(from module syllabus)**

- Demonstrate knowledge and critical understanding of innovation, creativity and enterprising mindset, recognising the values and the contribution creativity makes to the common good.
- Conceive, articulate and apply creative thinking within a work-based or academic context to develop novel solutions and/or value creation.

CyberAi

Introduction :

In today's technology-driven world, we are increasingly facing cybersecurity threats that traditional methods are struggling to combat. This is where CyberAI is a fusion of cybersecurity and artificial intelligence comes into place. By analysing attack patterns preemptively and intervening quickly, CyberAI uses the power of AI to learn and evolve from previous incidents. This proactive and adaptive approach to security allows us to stay one step ahead of threats, moving beyond reactive defense.

Task 1: Project Management:

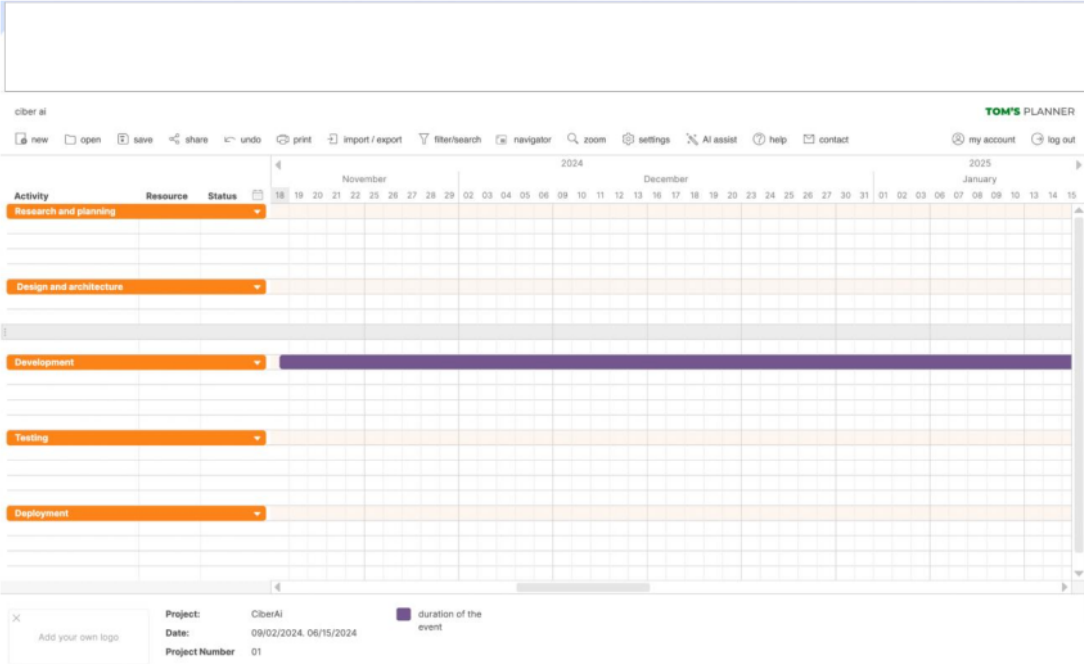
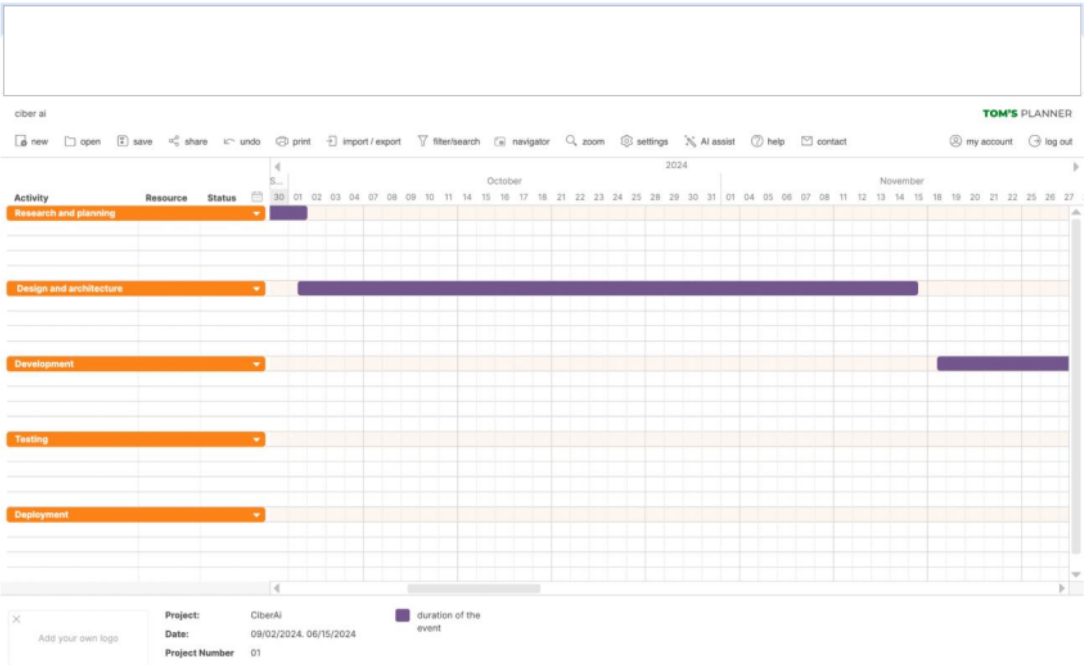
Q1 project management & planing

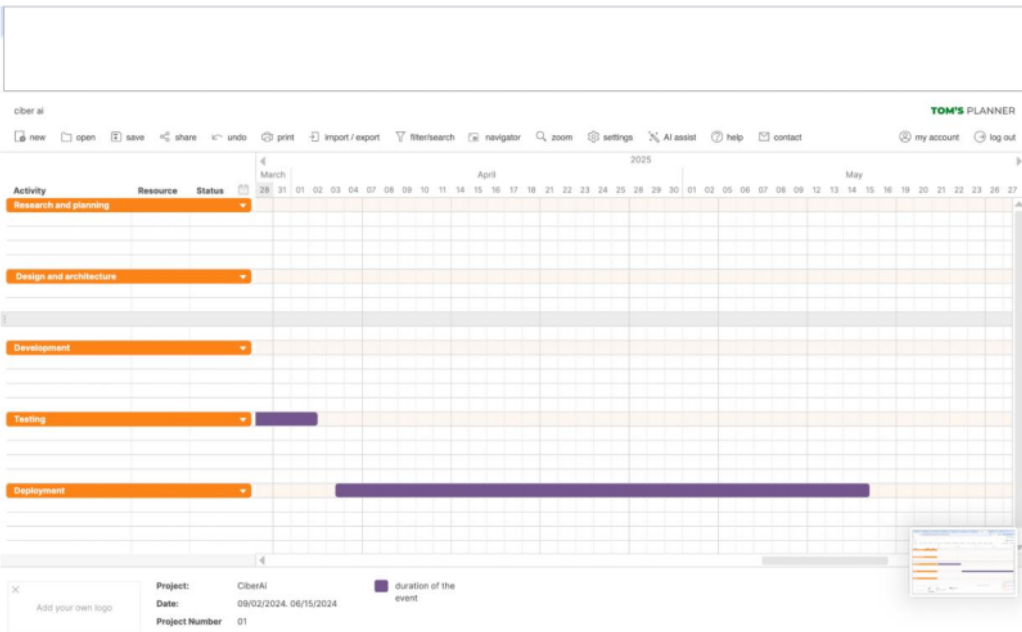
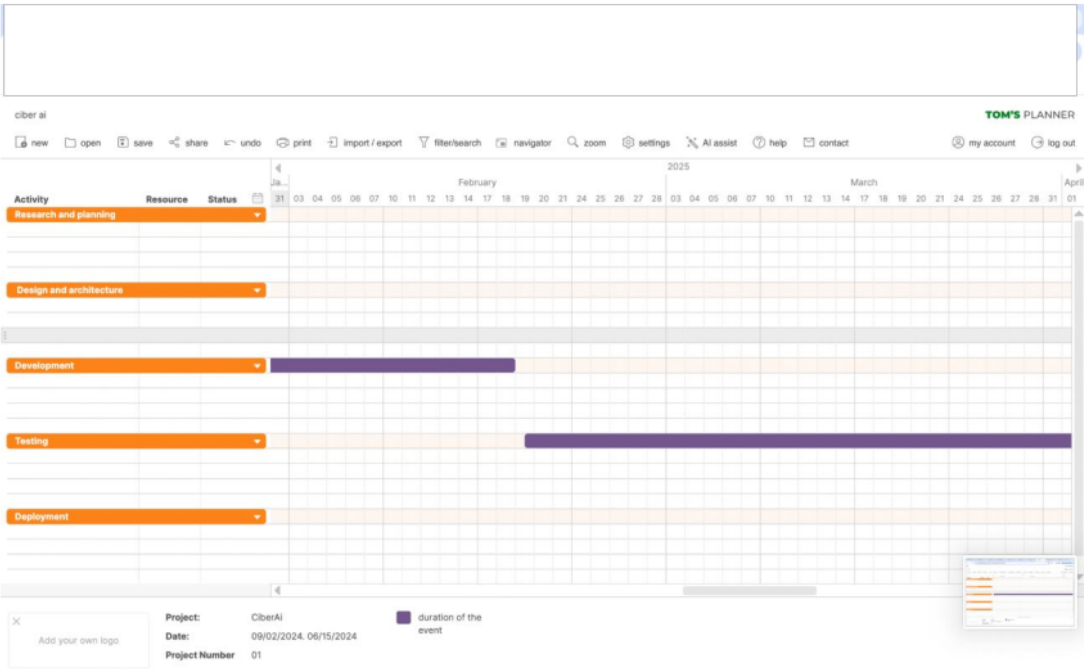
- **Aim/Idea/Problem:** The goal of this project is to create CyberAI, a technology that combines AI with cybersecurity to improve prevention, detection, and response. The concept comes from the limitations of current cybersecurity practices in dealing with increasingly complex cyber threats. Using AI algorithms, CyberAI aims to analyse attack patterns, and potential risks, and take measures to reduce threats before they happen. This approach aims to close the void between changing cyber threats and standard security measures, allowing companies to protect themselves from attacks and safeguard their digital assets
- **Proposed Solution:** The proposed solution would be a tool that combines natural language processing, deep learning, and machine learning to analyse cybersecurity data in real time. Its main function is to learn from previous accidents, evolve, and adapt to new threats on its own. It will also have a user-friendly interface so that the analysts can easily monitor its activities. This approach is designed to change cybersecurity by offering organizations a proactive defense system that can anticipate and respond to evolving threats using advanced AI-driven response capabilities and analysis
-

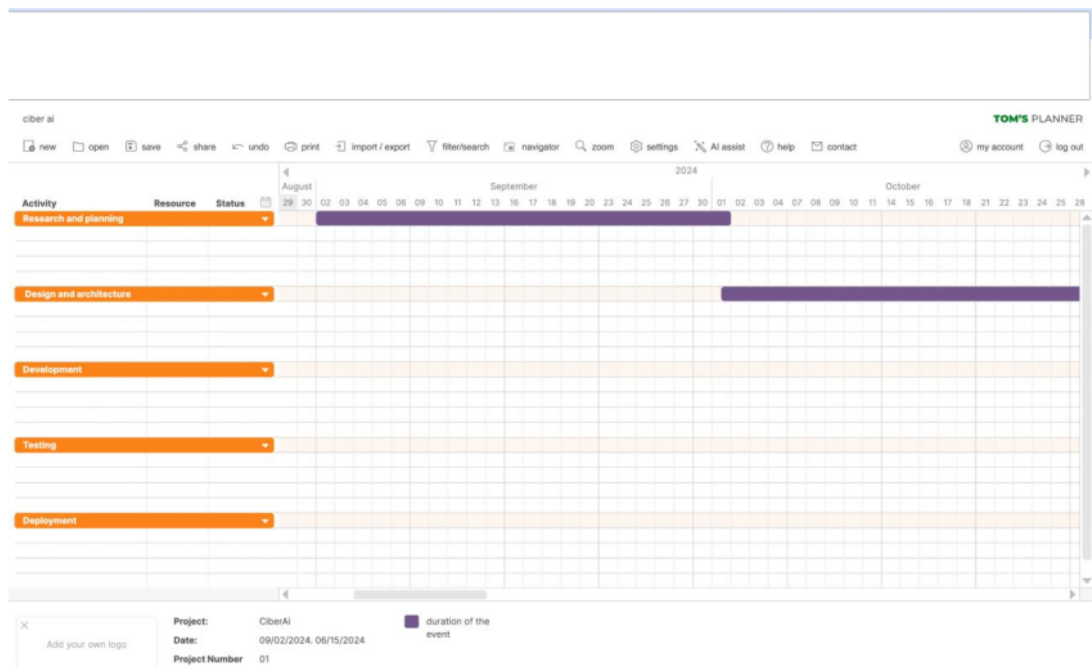
Programming languages	Python java
Ai frameworks	TensorFlow PyTorch
Data processing tools	Apache spark Hadoop
Cybersecurity tools	Prevention system intrusion detection SIEM solutions
Cloud infrastructure	AWS Azure
Human resource	Cybersecurity teacher, Ai teacher

- Key technologies and resources: Project timeline:** the goal is to work on CiberAi for 9 months
 Research and planning (1 month): The goal will be to find the project objective and scope, research the notions such as AI and cybersecurity, and identify the key tools needed such as the technologies and tools
 Design and architecture (1.5 months): the goal is to design CyberAi architecture, develop and collect data, and integrate autonomous response mechanisms
 Development (3 months): The goal is to implement an AI algorithm model develop the data collection pipeline and finally add the automotive response mechanism into the technology
 Testing (1 Month): the goal is to conduct a thorough testing for the AI algorithm, as well as a testing of the CiberAi and simulate a fake cyberattack to see if CiberAii works
 Deployment (1 month): The goal is to prepare all the documentation needed for CyberAi systems, deploy CiberAi in test evidence, and conduct a training session with an actual person
 Evaluation and optimisation (1 month): The goal is to monitor its performance, gather feedback from others and upgrade and optimize CiberAi based on the feedback
- Schedule and constraints:**
 To create cyberAi in nine months, weekly meetings are essential to follow up on progress and ensure everything is going at the right pace, respecting deadlines and seeing where we are in the project.
 However, some constrains might be budget constraints due to the need for new technologies and tools, potential delays due to possible technical challenges, and AI and cybersecurity regulation development process

• Gant charte :







- Development method :** When working on CyberAI project, we will use Agile methodologies such as Scrum or Kanban. These approaches provide the flexibility and adaptability needed to address the ever-changing cybersecurity threats landscape. Scrum divides the project into brief sprints, promoting iterative development and ongoing enhancement. It encourages teamwork and feedback, while Kanban focuses on visual management and consistent delivery, allowing us to monitor progress and deliver value steadily. By incorporating these methodologies, we can manage risks, and create a proactive and responsive CyberAI tool that evolves effectively.

Q2 project design

To explain the project design, i will explain to you how CiberAi works in a story :

Consider this: At the head office of your company, Monday morning is hectic. Workers are beginning their workday by logging in, and the IT department is preparing for a new week. The alert system of CyberAI suddenly flashes a red flag, signalling a possible cyberthreat. The AI algorithms identify anomalous network behaviour, such as an increase in data packets from an unidentified source trying to access private files stored in your business's database. CyberAI reacts fast, examining the incoming data and identifying the patterns of a highly skilled hacking attempt. CyberAI quickly executes its automatic answer without waiting for human participation. The suspicious IP address is isolated, preventing it from accessing any more information. It also turns on stronger security mechanisms at the same time, strengthening the firewall and encrypting important files to keep off unwanted access. CyberAI, in the meantime, instantly notifies the IT staff of the possible compromise. They leap into action, working with

CyberAI to evaluate the circumstances and put further safeguards in place. CyberAI keeps an eye on the network while the attack progresses, looking for any indications of additional intrusion. It instantly detects and eliminates new threats, avoiding any serious harm to the data or operations of your business. Following an attack, CyberAI creates a comprehensive report that describes the event, the steps that were taken, and suggestions for future prevention. After reading the report, the IT staff is better equipped to defend the company's cybersecurity posture and learn important lessons about the threat vectors. Because of CyberAI's proactive defence capabilities, a potentially disastrous cyberattack is effectively avoided by your firm. Knowing that the newest AI-driven cybersecurity technology is safeguarding your digital assets allows you to confront any cyber crisis with confidence when you have CyberAI on your side.

Task 2: Innovation:

Q1

- Cisco Systems Inc., a worldwide leader in networking and cybersecurity solutions, is operating in a constantly changing external landscape. This includes navigating diverse government regulations on data privacy and cybersecurity, as well as addressing issues related to international trade policies and government surveillance programs. Additionally, Cisco must also deal with economic fluctuations that impact IT spending, while actively pursuing opportunities in digital transformation projects. Socially, the company is dedicated to promoting diversity in the workforce and addressing the growing awareness of cybersecurity risks among consumers. Cisco relies on technologies such as networking and cloud computing to stay ahead, but must be cautious of ever-changing cybersecurity threats. Despite having a solid brand image and varied product lineup, Cisco struggles with pricing and reliance on hardware. Growth opportunities exist in 5G, IoT, and cloud services, yet competition, cybersecurity risks, and rapid technological changes pose significant threats. Ethically and legally, Cisco must adhere to data privacy laws, safeguard intellectual property, use AI responsibly, support environmental sustainability, and uphold ethical cybersecurity standards.

Q2

- Here is the plan we are putting in place to develop CyberAI within our organization. We will use agile development methodologies, DevOps practices, and CI/CD pipelines to ensure efficient development cycles. Our development process will involve using Scrum or Kanban for project management, holding regular stand-up meetings, and keeping a well-groomed backlog. Regarding deployment, we will be using Infrastructure as Code (IaC) principles and containerization with Docker or Kubernetes. Automated deployment and configuration management tools like Terraform and Ansible will play a key role. Proactive monitoring and incident management will be essential for maintenance. We will implement monitoring and logging using tools such as Prometheus or ELK stack, and create incident response protocols with PagerDuty or Opsgenie. Our approach will include ongoing enhancements through techniques like A/B testing and feature toggles, driven by customer feedback analysis and performance evaluations. We will incorporate

cybersecurity measures like vulnerability assessments and security incident response, utilizing tools like Splunk or Elastic Security. Lastly, in terms of AI integration, our focus will be on model training, data pipelines, and monitoring, using TensorFlow or PyTorch for deep learning and Apache Spark or Hadoop for data processing. With our thorough strategy, we will guarantee that CyberAI is created, rolled out, upheld, and advanced successfully in our company, helping us stay at the forefront of cybersecurity

Task 3: Project reflection:

- By developing CiberAi i will have the chance to expand my skill set into different areas. I will continue sharpening my technical knowledge with advanced Python and Java coding in addition to implementing AI frameworks like TensorFlow or PyTorch. Furthermore, I aim at mastering Apache Spark/Hadoop that are not only used for big data processing but also understanding how Amazon Web Services and Microsoft Azure operate within cloud infrastructure. My goal is obtaining better understanding on implementation defenses against hacking attacks or unauthorized access into data systems including prevention systems, intrusion detection systems as well as SIEM solutions through this project emphasis on cybersecurity tools and practices. Thi project will significantly enhance my skills through not only improvement of technical capabilities but also integration of other themes such as innovations among others from diverse disciplines into AI-oriented information security.
- Enhancing cybersecurity measures, this project and the new talents it produces can have a major positive impact on society. The development of CyberAI, which combines cybersecurity and artificial intelligence, fortifies defences against cyberthreats by anticipatorily identifying attack patterns and lowering the likelihood of cyberattacks on people, companies, and vital infrastructure. CyberAI reduces the financial and psychological effects of data breaches by safeguarding digital assets and sensitive information, such as intellectual property and personal data. This promotes trust in online communication channels and digital transactions. CyberAI also helps to maintain data privacy standards, protect people's right to privacy in a time when privacy is of utmost importance, encourage digital inclusion, and make it possible for more people to take advantage of digital technology. In conclusion yess CiberAi does have a positive impact but like all technologie it can be used for good or for bad
- The CyberAI project faces several risks and challenges that need to be addressed to ensure its success. The technical complexity of creating AI-driven cybersecurity solutions is a major obstacle, but it may be lessened with careful design, study, and regular expert input. Additionally, important are data security and privacy, which call for strong defences like encryption and adherence to laws like the GDPR. Another risk associated with integration with current infrastructure is minimised by compatibility tests and evaluations. Resource limitations might impede growth, therefore setting priorities and creating a reasonable budget are necessary. Constant observation and legal advice are necessary to ensure compliance with changing rules. Testing on a regular basis and

using secure coding techniques are necessary to mitigate cybersecurity threats, including vulnerabilities. Incorporating end users into the design process and offering them thorough training are the final steps in guaranteeing user acceptability. By taking preemptive measures to mitigate these risks, the CyberAI project can move on without incident and successfully accomplish its goals.

Conclusion

In conclusion, the CyberAI project offers a stimulating chance to design a novel approach that integrates cybersecurity and artificial intelligence to build a preventative defence system. CyberAI attempts to efficiently safeguard digital assets and lessen cyber dangers by anticipating attack trends and acting swiftly. Throughout the project, our main goal will be to acquire new technical abilities in big data processing, cloud infrastructure, AI frameworks, Python, Java, and cybersecurity technologies. Moreover, abilities, promote creativity, and expand multidisciplinary knowledge. Although there will always be risks and difficulties, we have provided thorough mitigation techniques to deal with them. In the end, a safer, more secure, and inclusive digital society will benefit from the effective development and application of CyberAI, enabling people and organisations to effectively protect against ever-evolving cyber threats.

FINAL GRADE

GENERAL COMMENTS

59/100

Total:		59
1. Engagement with Literature Skills:		
- No use of citations. No reference list.	20	0
2. Knowledge and Understanding Skills: 10, 10		
* Project Man. & Planning: + Evidence of knowledge and skills covering project scope inc. proposed solution, required Technologies/resources to be used, a project timeline schedule & Gantt chart documented. Good. + ii: Appropriate concepts, methods, practices and tools to develop, deploy, maintain and evolve the practical element of the project is considered and documented. – could be supported by citations.	20	18
3. Cognitive and Intellectual Skills: 5e		
+ Development methodology and Project scope assessed and documented. +/- PEST & SWOT analysis summary includes some key considerations and documents some legal & ethical considerations. – Summary could be structured using the EST and SWOT framework and additional professional legal & ethical considerations documented. + Project's positive impact on society is clearly described.	20	16

+ Potential risks identified, and contingencies documented. Good. – Could be documented in a risk analysis table to enhance format, presentation, and readability.		
4. Practical Application Skills: 10, 10		
* Gantt chart: + Gantt chart is clearly structured. – could also include more specific schedule tasks. * Project Design: +/- 1 piece of design work related to the practical element of the project has documented via a story. Good. – Some visuals could be used an additional design artifact documented.	20	12
5. Transferable Skills for Life and Professional Practice: 5, 15		
New skills: + Potential to develop new skills clearly documented. Good. – Some additional soft skills could be identified. Report: Report structure, format and presentation quite good. – Could be enhanced in 1/2 areas: – No title page and Toc. – Try to avoid using 'I' when writing a report. And use third person tense instead. – Minor spelling and grammar errors in places. – On-time and plagiarism check: /	20	13

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10
