|  |
| --- |
| **ĐẠI HỌC QUỐC GIA HÀ NỘI**  Ảnh có chứa văn bản, biểu tượng, vòng tròn, Phông chữ  Nội dung do AI tạo ra có thể không chính xác.**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ**  **BÁO CÁO DỰ ÁN CÔNG NGHỆ**  **Ngành: Trí tuệ nhân tạo**  **ỨNG DỤNG CÁC MÔ HÌNH NGÔN NGỮ LỚN**  **TRONG PHÁT HIỆN CÁC BẤT THƯỜNG VỀ**  **NGỮ NGHĨA TRONG QUY TRÌNH KINH DOANH**    **Sinh viên : Bùi Thế Long**  **Mã sinh viên : 22022647**  **Lớp : K67I-AI1**  **Giảng viên hướng dẫn : Th.S.Nguyễn Thùy Linh** |

Ý kiến đánh giá: ................................................................................................................

............................................................................................................................................

............................................................................................................................................

............................................................................................................................................

............................................................................................................................................

Điểm số: .................................................... Điểm chữ: ................................................

*Hà Nội, ngày 10 tháng 5 năm 2024*

Giảng viên đánh giá

*(Ký, ghi rõ họ tên)*

**MỤC LỤC**

[I. GIỚI THIỆU 4](#_Toc197800411)

[II. KIẾN THỨC NỀN TẢNG 4](#_Toc197800412)

[1. Object-centric Process Mining 4](#_Toc197800413)

[2. Object-centric Anomaly Detection 5](#_Toc197800414)

[3. Các cấp độ của bất thường 5](#_Toc197800415)

[III. CÔNG TRÌNH LIÊN QUAN 6](#_Toc197800416)

[1. Phương pháp thống kê (Statistical-based Methods) 6](#_Toc197800417)

[2. Phương pháp dựa trên ngữ nghĩa (Semantic-based Methods) 7](#_Toc197800418)

[3. Phương pháp kiểm tra sự phù hợp (Conformance Checking-based Methods) 7](#_Toc197800419)

[IV. PHƯƠNG PHÁP 8](#_Toc197800420)

[1. Chuẩn bị dữ liệu 8](#_Toc197800421)

[2. Câu hỏi Prompt và nội dung trả lời 10](#_Toc197800422)

[3. Mô hình ngôn ngữ lớn – Llama-3.1-8B 10](#_Toc197800423)

[4. Fine-tune 11](#_Toc197800424)

[V. KẾT QUẢ ĐẠT ĐƯỢC VÀ HƯỚNG PHÁT TRIỂN TIẾP THEO 11](#_Toc197800425)

[VI. KẾT LUẬN 12](#_Toc197800426)

[THAM KHẢO 12](#_Toc197800427)

# I. GIỚI THIỆU

Việc phát hiện các bất thường trong quy trình nghiệp vụ đóng vai trò quan trọng nhằm đảm bảo hoạt động ổn định và hiệu quả. Các phương pháp truyền thống thường dựa trên tần suất thống kê, nhưng cách tiếp cận này có hạn chế vì không phải mọi hành vi hiếm gặp đều là không mong muốn. Thay vào đó, phân tích từ góc độ ngữ nghĩa giúp phát hiện bất thường chính xác hơn. Tuy nhiên, các phương pháp hiện có thường chia nhỏ quy trình thành các cặp sự kiện, dẫn đến mất thông tin về các phụ thuộc dài hạn.

Trong báo cáo này, em sẽ trình bày quá trình tái triển khai phương pháp DABL (Detecting Anomalies in Business Processes using LLMs) từ nghiên cứu gốc [1], với điều chỉnh sử dụng mô hình ngôn ngữ Llama 3.1-8B thay vì Llama 2-13B để phù hợp với khả năng tính toán. Mục tiêu của em là chạy lại thử nghiệm với phiên bản mô hình nhỏ hơn nhưng vẫn đảm bảo khả năng phát hiện bất thường ngữ nghĩa, đánh giá hiệu quả của mô hình sau khi fine-tune trên tập dữ liệu gồm 20.000 quy trình nghiệp vụ được mô phỏng từ dữ liệu thực tế và cuối cùng là kiểm tra khả năng ứng dụng trên các tập dữ liệu khác nhau.

Cấu trúc báo cáo: Phần 2: Kiến thức nền tảng. Phần 3: Các phương pháp liên quan. Phần 4: Phương pháp. Phần 5: Kết quả thử nghiệm và hướng phát triển. Phần 6: Kết luận và đánh giá.

Bằng cách tối ưu hóa quy trình huấn luyện với mô hình nhỏ gọn hơn, nghiên cứu này góp phần mở rộng khả năng ứng dụng DABL trong điều kiện tài nguyên hạn chế mà vẫn duy trì hiệu quả đáng kể.

# II. KIẾN THỨC NỀN TẢNG

## 1. Object-centric Process Mining

**Object-centric Process Model** là một phương pháp mở rộng của Process Mining, thay vì gán mỗi sự kiện với một case ID duy nhất, nó cho phép **sự kiện liên kết với nhiều đối tượng (objects) khác nhau**:

* Mỗi object có vòng đời riêng biệt.
* Một sự kiện có thể liên quan đến nhiều object.
* Thay vì chỉ phân tích chuỗi sự kiện theo case ID, OCPM xem xét mạng lưới mối quan hệ giữa các đối tượng.

Các phương pháp PM truyền thống thường dựa vào event logs có cấu trúc đơn giản, với mỗi sự kiện được liên kết với 1 case ID duy nhất.

* Tuy nhiên, trong thực tế, nhiều quy trình liên quan đến nhiều đối tượng (objects) tương tác với nhau, làm cho mô hình trở nên hạn chế
* Ví dụ, trong quản lý chuỗi cung ứng:
  + 1 đơn hàng có thể có nhiều sản phẩm.
  + 1 sản phẩm có thể được liên kết với nhiều nhà cung cấp.
  + 1 hóa đơn có thể thanh toán nhiều sản phẩm khác nhau.

## 2. Object-centric Anomaly Detection

**Object-centric Anomaly Detection** là 1 phương pháp **phát hiện bất thường trong dữ liệu sự kiện theo hướng đối tượng** (object-centric event data) mà không cần phải xây dựng mô hình quy trình object-centric trước đó.

Các phương pháp process mining truyền thống hay rule-based anomaly detection thường giả định có 1 quy trình chuẩn (gọi là de-jure model) sau đó so sánh dữ liệu thực tế với mô hình này để tìm bất thường, tuy nhiên cách tiếp cận này sẽ gặp khó khăn khi:

* Dữ liệu quá phức tạp để mô hình hóa trước.
* Nhiều đối tượng (objects) tương tác với nhau, làm cho việc xây dựng mô hình trở nên khó khăn.
* Bất thường có thể xảy ra ở cấp độ đối tượng chứ không chỉ ở cấp độ sự kiện hoặc quy trình.

## 3. Các cấp độ của bất thường

**3.1. Cấp độ sự kiện (Event-level Anomaly)**

* Khi 1 sự kiện có thông tin hoặc hành vi không bình thường so với các sự kiện khác trong cùng loại quy trình.
* Ví dụ:
  + Một giao dịch thanh toán có số tiền âm.
  + Một nhân viên đăng nhập vào hệ thống lúc 3 giờ sáng (ngoài giờ làm việc).
  + Một đơn hàng được vận chuyển trước khi được xác nhận thanh toán.
* **Nhận diện: So sánh từng sự kiện với mẫu chuẩn (normal behavior) và chỉ mang tính chất đơn lẻ.**

**3.2. Cấp độ quy trình (Process-level Anomaly)**

* Khi toàn bộ quy trình (chuỗi các sự kiện) diễn ra theo cách không bình thường
* Ví dụ:
  + Một yêu cầu bảo hiểm được xử lý nhanh hơn gấp 10 lần bình thường (có thể có nhiều lỗi sai).
  + Một bệnh nhân thực hiện xét nghiệm trước khi đăng kí khám bệnh (làm sai từ bước bắt đầu → sai cả quy trình về sau).
* **Nhận diện: So sánh toàn bộ trình tự (sequence) của quy trình với các quy trình thông thường.**

**3.3. Cấp độ đối tượng (Object-level Anomaly)**

* Khi 1 đối tượng có đặc điểm hoặc hành vi tổng thể khác biệt so với các đối tượng khác cùng hệ thống.
* Ví dụ:
  + Một khách hàng thực hiện số lượng giao dịch gấp 10 lần trung bình.
  + Một sản phẩm trong kho có số lần xuất kho bất thường.
  + Một tài khoản nhân viên liên quan đến quá nhiều sự kiện cùng lúc (có thể bị tấn công).
* **Nhận diện: So sánh toàn bộ dữ liệu liên quan đến 1 object so với các object khác.**

# III. CÔNG TRÌNH LIÊN QUAN

## 1. Phương pháp thống kê (Statistical-based Methods)

* **Nguyên lý:** Phân tích tần suất thống kê của các dấu vết (traces) để xác định điểm bất thường.
* **Cách tiếp cận:**
  + Mô hình xác suất: Sử dụng Markov Chains, Bayesian Networks để ước tính xác suất của một trace (VD: HPDTMC, EDBN, PN-BBN).
  + Biểu diễn vector & khai thác dữ liệu: Ánh xạ traces thành vector rồi áp dụng các thuật toán như LOF, Isolation Forest, Word2Vec, Trace2Vec.
  + Học sâu: Dùng Autoencoder với LSTM/GRU hoặc Graph Neural Networks (GNNs) để phát hiện bất thường qua lỗi tái tạo (reconstruction error).
* **Hạn chế:** Không phải hành vi hiếm gặp nào cũng là bất thường, và hành vi phổ biến cũng không phải lúc nào cũng bình thường.

## 2. Phương pháp dựa trên ngữ nghĩa (Semantic-based Methods)

* **Nguyên lý:** Sử dụng phân tích ngữ nghĩa để xác định xem hành vi có phù hợp với logic nghiệp vụ hay không.
* **Cách tiếp cận:**
  + Dùng mô hình ngôn ngữ (BERT, GloVe, SVM) để phân tích tên hoạt động và trích xuất động từ - đối tượng nghiệp vụ.
  + Xây dựng cơ sở tri thức (knowledge base) để kiểm tra xem hành vi có vi phạm các quy tắc logic nghiệp vụ không.
  + Một số phương pháp phân tích cặp sự kiện (event pairs) để xác định bất thường.
* **Hạn chế:**
  + Không nắm bắt được mối quan hệ xa (long-distance dependencies) giữa các sự kiện.
  + Chủ yếu tập trung vào các cặp sự kiện đơn lẻ, khiến việc hiểu nguyên nhân bất thường khó khăn hơn.

## 3. Phương pháp kiểm tra sự phù hợp (Conformance Checking-based Methods)

* **Nguyên lý:** So sánh traces với mô hình quy trình chuẩn để phát hiện sai lệch.
* **Cách tiếp cận:**
  + Xây dựng mô hình quy trình (do người dùng cung cấp hoặc khai thác từ event log).
  + Dùng các kỹ thuật kiểm tra sự phù hợp (conformance checking) để đánh giá độ lệch giữa dấu vết và mô hình quy trình.
* **Hạn chế:**
  + Phụ thuộc vào chất lượng của mô hình quy trình.
  + Khó áp dụng cho quy trình phức tạp do khó mô hình hóa chính xác.

# IV. PHƯƠNG PHÁP

## 1. Chuẩn bị dữ liệu

Để có thể fine-tune hiệu quả các LLM để tạo ra 1 mô hình chung có khả năng xác định được các sự bất thường về mặt ngữ nghĩa (semantic anomalies) trong quy trình kinh doanh, một log bắt buộc phải có những đặc điểm sau:

* Nó phải bao gồm các normal và anomalous traces.
* Nó phải chứa các thông tin ngữ nghĩa phong phú (ví dụ: 1 hoạt động không nên được biểu diễn bởi những kí tự vô nghĩa).
* Các traces lấy từ nó phải bắt nguồn từ nhiều quy trình khác nhau trên nhiều miền khác nhau.

Những process model này trải dài trên nhiều miền, liên quan đến các quy trình thông thường (hóa đơn, xử lý yêu cầu,…), cũng như các quy trình chuyên biệt từ công nghệ phần đến lĩnh vực y tế. Từ đó, tổng hợp nên các trace thông thường

**1.1. Tạo các bộ Normal Traces**

* Từ các bộ dữ liệu từ các tài liệu trên, process model được tổng hợp nên và bao gồm các đặc điểm sau:
  + Đều được kí hiệu bằng Business Process Modeling Notation.
  + Miêu tả bằng tiếng anh.
  + Và chuyển đổi thành 1 mạng workflow hợp lý (sound).
* Kết quả là tập hợp của … process model và bao gồm … traces thông thường. Trong khi đó vẫn giữ lại 1,000 process model để tạo ra các bộ dữ liệu test.
* Với mỗi process model chúng ta có được 1 tập hợp các normal trace kí hiệu là .
* Để ngăn việc các trace này loop mãi mãi, nghĩa là độ dài trace là infinite, mỗi process model chỉ được lặp lại 2 lần.

**1.2. Tạo các bộ giả lập các Anomaly Traces**

Các normal trace có thể chuyển thành các anomalous traces bằng 2 cách:

**1.2.1. Ordering Anomalies**

* Làm gián đoạn thứ tự xử lý các hành động, nghĩa là đúng ra các hoạt động này phải được thực thi theo 1 chuỗi khác.
* Tuy nhiên việc tạo ra các bộ anomalies vẫn có xác suất tạo nên 1 bộ normal trace, nên vì thế với mỗi process model , chúng ta sẽ tạo được 1 bộ ordering anomalies và loại trừ các trường hợp từ bộ normal trace .
* Năm loại của Ordering Anomalies:

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, hàng

Nội dung do AI tạo ra có thể không chính xác.

**1.2.2. Exclusion Anomalies**

* Xảy ra khi 2 hành động trên nhánh exclusive (nghĩa là làm hành động này hoặc hành động kia) cùng được thực thi
* Như process model ở trên sau khi được biểu diễn bằng 1 process tree, ta có thể hình dung việc tạo 1 bộ anomalies bằng cách thay thế transition exclusive bằng transition song song .
* Từ đó, các hành động đúng ra phải được thực thi 1 cách riêng rẽ thì nay sẽ được thực thi 1 cách song song
* Từ bộ anomalies và loại trừ đi các trường hợp của bộ normal traces , ta có được 1 bộ anomalies hoàn chỉnh .

Ảnh có chứa văn bản, biểu đồ, hàng, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

## 2. Câu hỏi Prompt và nội dung trả lời

* Để tiến hành prompt fine-tune trên LLM, 1 bộ truy vấn văn bản tương ứng (corresponding textual queries) dựa trên các bộ anomalies.
* Mỗi truy vấn này bao gồm 2 thành phần:
  + Thành phần đầu tiên là các traces, như là

“Is this following business process trace, each executed activity is separated by a comma: [Send acceptance pack, Check credit history, Assess loan risk, Assess eligibility, Prepare acceptance pack]”.

* + Thành phần thứ 2 là câu hỏi xem là trace này có phải anomalous hay không:

“Is this trace normal or anomalous?”.

* Nếu mà là anomalous thì model sẽ được hỏi về nguyên nhân gây ra bất thường:

“What causes this trace to deviate?”.

“The activity ’Send acceptance pack’ is executed too early, it should be executed after ’Prepare acceptance pack’.”.

## 3. Mô hình ngôn ngữ lớn – Llama-3.1-8B

DABL sử dụng **Unsloth**, một thư viện tối ưu hóa tinh chỉnh LLMs, thay thế cho QLoRA (Dettmers et al. 2024) trong bài báo gốc. Unsloth được thiết kế để tăng tốc độ và giảm chi phí tính toán khi tinh chỉnh các mô hình ngôn ngữ lớn, đặc biệt phù hợp với các mô hình như Meta-Llama-3.1-8B. DABL tinh chỉnh unsloth/Meta-Llama-3.1-8B để khắc phục thiếu hụt kiến thức chuyên môn, tận dụng khả năng hiểu ngữ nghĩa và phụ thuộc dài hạn để phân tích trace.

* **Unsloth là gì?**: Unsloth là một thư viện mã nguồn mở tối ưu hóa hiệu suất tinh chỉnh LLMs, giúp tăng tốc độ huấn luyện lên đến 2-5 lần và giảm sử dụng bộ nhớ GPU so với các phương pháp truyền thống. Nó sử dụng các kỹ thuật như lượng tử hóa (quantization), tối ưu hóa kernel, và quản lý bộ nhớ hiệu quả.

**Ưu điểm của Unsloth trong DABL**:

* **Hiệu suất cao**: Unsloth tối ưu hóa quá trình tinh chỉnh Meta-Llama-3.1-8B, một mô hình 8 tỷ tham số, giúp giảm thời gian huấn luyện trên tập dữ liệu lớn.
* **Tiết kiệm tài nguyên**: Bằng cách sử dụng lượng tử hóa 4-bit và các kỹ thuật tối ưu hóa khác, Unsloth giảm yêu cầu bộ nhớ GPU, cho phép tinh chỉnh trên phần cứng mà không cần tài nguyên quá lớn.
* **Tương thích với mô hình hiện đại**: Unsloth hỗ trợ các mô hình tiên tiến như Meta-Llama-3.1-8B, được thiết kế với kiến trúc Transformer cải tiến, mang lại hiệu suất vượt trội so với Llama 2-Chat 13B trong bài báo gốc.
* **Dễ tích hợp**: Unsloth tích hợp dễ dàng với các công cụ như PyTorch và Hugging Face Transformers, cho phép DABL sử dụng các trình tối ưu hóa.

## 4. Fine-tune

Để thực nghiệm finetuning với Meta-Llama-3.1-8B, các cấu hình sẽ được thay đổi như sau:

* Bộ dữ liệu: Bộ dữ liệu thực nghiệm chứa 19.200 traces được lấy ngẫu nhiên từ các traces trong bộ dữ liệu gốc để giảm khối lượng tính toán và phù hợp với nhiệm vụ thực nghiệm.
* GPU: Mô hình sẽ được finetune trên GPU Tesla T4 16GB của google colab.
* Cấu hình fine tune:

Ảnh có chứa văn bản, Phông chữ, ảnh chụp màn hình

Nội dung do AI tạo ra có thể không chính xác.

* Cài đặt cấu hình sinh câu trả lời của mdel PEFT: Mô hình sử dụng cấu hình high quality search thay vì chỉ sử dụng beam search như mô hình gốc vì chỉ được finetune trên lượng dữ liệu nhỏ, mô hình chưa học được đủ. Cấu hình sử dụng top\_k = 50 thay vì 5 như trước và thêm top\_p là nucleus sampling lấy token trong khối xác suất tích lũy 90%, temperature = 0.1 giới hạn mức độ ngẫu nhiễn trong đầu ra của mô hình để hạn chế mô hình đưa ra câu trả lời không chính xác và repetition\_penalty = 1.1 giúp giảm lặp từ trong câu trả lời.
* Link Colab:

https://colab.research.google.com/drive/1xVV2O26x9KaBTtS5OefiDTmMggF5S7Ko?usp=sharing

# V. KẾT QUẢ ĐẠT ĐƯỢC VÀ HƯỚNG PHÁT TRIỂN TIẾP THEO

Do giới hạn về thiết bị nên mô hình chỉ được finetune trên một lượng dữ liệu tương đối nhỏ, vì vậy câu trả lời của mô hình không có cấu trúc cố định và còn nhầm lẫn giữa các trace bình thường và bất thường. Bên cạnh đó, vẫn có lỗi đầu ra với những trace trong bộ test được sinh từ các mô hình quy trình mà mô hình chưa được huấn luyện. Một số câu trả lời của mô hình:

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, màu đen

Nội dung do AI tạo ra có thể không chính xác.

Ảnh có chứa ảnh chụp màn hình, văn bản, Phông chữ, màu đen

Nội dung do AI tạo ra có thể không chính xác.

# VI. KẾT LUẬN

Dự án “Ứng dụng mô hình ngôn ngữ lớn trong phát hiện bất thường khai phá quy trình” (DABL) mà em trình bày trong báo cáo này đã đề xuất một hướng tiếp cận mới nhằm nâng cao hiệu quả phát hiện và giải thích các bất thường ngữ nghĩa trong quy trình kinh doanh thông qua việc sử dụng mô hình ngôn ngữ lớn (LLM), cụ thể là Meta-Llama-3.1-8B được tinh chỉnh bằng Unsloth.

Khác với các phương pháp truyền thống vốn gặp nhiều hạn chế trong việc nắm bắt ngữ nghĩa và phụ thuộc dài hạn, phương pháp của dự án đã tận dụng khả năng hiểu ngôn ngữ tự nhiên và cấu trúc chuỗi sự kiện của LLM để cải thiện độ chính xác và khả năng giải thích bất thường. Việc xây dựng bộ dữ liệu tổng hợp lớn và đa dạng từ hơn 143.000 mô hình quy trình thực tế, cùng với kỹ thuật sinh bất thường có hệ thống, đã đóng vai trò quan trọng trong việc huấn luyện và đánh giá mô hình. Kết quả thực nghiệm dù còn hạn chế do tài nguyên tính toán chưa đủ mạnh, nhưng bước đầu cho thấy tiềm năng rõ rệt của phương pháp này trong việc phát hiện và lý giải bất thường.

Thông qua quá trình thực hiện dự án, em đã có cơ hội tiếp cận sâu hơn với lĩnh vực khai phá quy trình và các mô hình ngôn ngữ lớn. Việc tìm hiểu về kiến thức của một đề tài mới như khai phá quy trình đã giúp em hiểu rõ hơn về quy trình nghiên cứu, từ việc đặt vấn đề, xử lý dữ liệu cho đến triển khai thực nghiệm và đánh giá kết quả. Đồng thời dự án cũng trang bị thêm cho em những kiến thức về finetune mô hình ngôn lữ lớn cho một đề tài hoàn toàn mới. Mặc dù gặp không ít khó khăn về mặt kỹ thuật và hạn chế thiết bị, em cảm thấy rất hài lòng vì đã có thể áp dụng kiến thức lý thuyết vào một chủ đề thực tiễn, mang tính ứng dụng cao. Dự án không chỉ giúp em nâng cao kỹ năng nghiên cứu và tìm hiểu các kiến thức mới mà còn rèn luyện tư duy hệ thống, tính kiên trì và cẩn trọng trong từng bước triển khai. Đây là một trải nghiệm học tập quý giá mà em sẽ ghi nhớ và tiếp tục phát triển trong những nghiên cứu sau này.

# THAM KHẢO

1. Nghiên cứu gốc: Wei Guan, Jian Cao, Jianqi Gao, Haiyan Zhao, Shiyou Qian:DABL: Detecting Semantic Anomalies in Business Processes Using Large Language Models  
   https://arxiv.org/pdf/2406.15781v1
2. Alessandro Berti 1,2 , Urszula Jessen 3,4 , Wil M.P. van der Aalst 1,2 and Dirk Fahland 4: Explainable Object-Centric Anomaly Detection: the Role of Domain Knowledge  
   <https://ceur-ws.org/Vol-3758/paper-30.pdf>