



RAFM

Working Group

GNERATE

Graph NEural network for financial
crime & fRAud SyndicaTE detection

Executive Summary

Indonesia mengalami **pertumbuhan ekonomi digital** *Year-on-Year* (YoY) sebesar **8%** setiap tahunnya (*ekon.go.id*, 2024). Ini memungkinkan terjadinya **perubahan perilaku bertransaksi** di masyarakat. Namun di sisi lain, pertumbuhan tersebut diiringi dengan **meningkatnya risiko kejahatan** di dunia maya khususnya pada kejahatan keuangan serta **fraud**.

Peraturan Bank Indonesia mengenai Perusahaan Jasa Pembayaran (PBI PJP 23/6/PBI/2021) memandatkan institusi keuangan untuk memiliki ***Fraud Management System***, sebagaimana dimaksud dalam Pasal 10, 14 dan 28 dalam hal kecukupan ketersediaan teknologi pendukung. Ketersediaan teknologi tersebut juga merupakan salah satu prasyarat izin beroperasinya suatu entitas keuangan.

Proyek ini bertujuan untuk mengembangkan dan menguji metode untuk **mendeteksi kejahatan terorganisir, sindikat fraud**, serta skema **Pencucian Uang** dalam ekosistem yang telah mengalami **digitalisasi**.

GENERATE menggabungkan analisis **Graph** serta **AI/ML** yang dilatih berdasarkan *real-life cases* menggunakan ***Heterogeneous Graph Transformation*** (HGT), ***Graph Statistics*** (*Centrality Measures and Community Detection*), serta ***Gradient Boosting Model*** (GBM) untuk menghasilkan model pendeteksian sindikat penipuan dan kejahatan terorganisir.

Frameworks yang kami susun sangat mungkin untuk diimplementasi baik di sektor industri maupun sebagai pelengkap infrastruktur keuangan elektronik nasional guna meningkatkan perlindungan, integritas, dan keamanan nasabah dan transaksi digital.

Tentang Kami

RAFM

Working Group




Lalu Garin Alham

Team Leader – Fraud & AML, & Data
7 tahun pengalaman di bidang Anti-Fraud & Anti-Money Laundering dengan pengalaman sebelumnya di Lembaga Penegak Hukum.

Tersertifikasi *Fraud Examiner* dan *Forensic Audit*.

 [Garin A](#)

 [researchgate/Lalu-Garin-Alham](#)



Ferdi Hidayat Irawandi

Team member – Fraud & Security
6+ tahun pengalaman di bidang Anti-Fraud. Pengalaman sebelumnya meliputi e-commerce serta *FinTech*

 [Ferd Hidayat I](#)



Kristy Natasha Yohanes

Team member – Fraud Analytics & AI/ML
Memiliki *repertoire* AI/ML beragam meliputi Machine Learning, Graph Theory, serta Computer Vision.

 [Kristy Natasha](#)

 [github/natgluons](#)



Nadirah Syahnas Sudarto

Team member – Risk & Business Assessor
6 tahun pengalaman di berbagai *digital company*, *FinTech*, & startup pada bidang Risk dan *Business Intelligence*.

Tersertifikasi di bidang *Risk Management*

 [Nadirah Sudarto](#)

Objektif.

1.

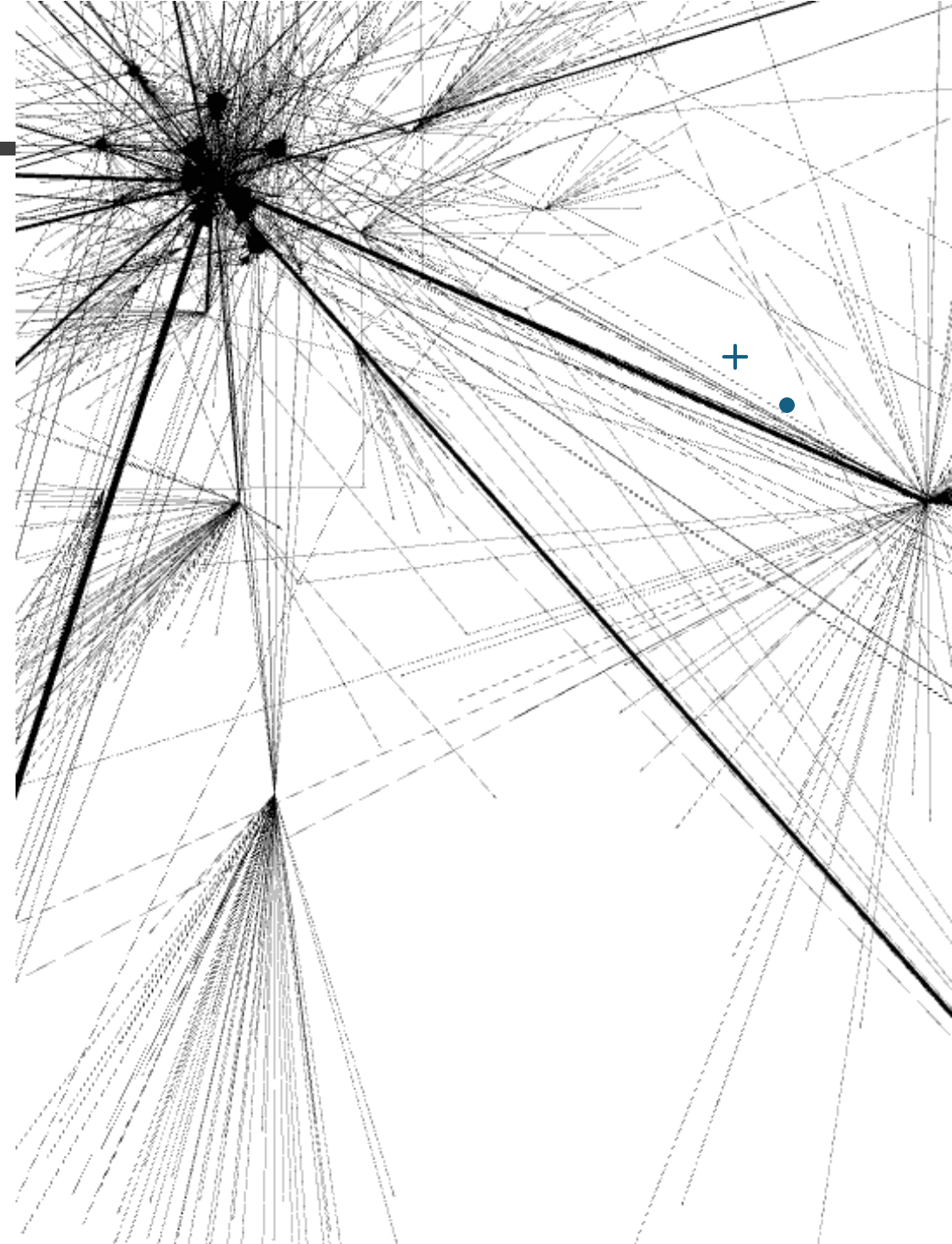
Menguji dan merumuskan pendekatan multi-spektrum untuk memahami perilaku **fraud & kejahatan terorganisir** di ekosistem keuangan digital.

3.

Membantu mewujudkan **inklusi keuangan** Indonesia yang mengedepankan **perlindungan, keamanan & kepercayaan pengguna** melalui upaya kolaboratif **pencegahan fraud & kejahatan terorganisir** dan pemberantasan TPPU.

2.

Mengembangkan dan mengimplementasi *framework* berbasis **Graph** dan **AI/ML** untuk **mendeteksi sindikat kejahatan keuangan** secara terintegrasi.



Rumusan Masalah: **Ekonomi Digital & *Konsekuensinya***

Pertumbuhan Transaksi **QRIS**

▲ **104%** ➡
YoY 2023 to 2022

Peredaran uang elektronik yang semakin besar
Allowing more crimes to take place online

Pertumbuhan Pengguna **QRIS**

▲ **~74%** ➡
YoY 2023 to 2022

Semakin banyak populasi masyarakat ke ekosistem digital
More difficulty & less visibility to detect crimes conducted by groups

Pertumbuhan Merchant **QRIS**

▲ **~40%** ➡
YoY 2023 to 2022

Kanal *cash-out* & use-case yang semakin kompleks
Enabling fraudsters to poach their victims from multiple approaches

Transaksi Fraud meningkat hingga 17% dari 2022 hingga 2023

Mastercard (2024)

Pelaku fraud **berevolusi**, dalam hal **Modus Operandi & Attack vector**

Europol (2023)

Pelaku kejahatan keuangan kemungkinan besar **bekerjasama** & memiliki **jaringan spesialisasi** tersendiri

FATF (2023)

Dibutuhkan solusi pengelolaan risiko fraud melampaui **rule-based** atau **monitoring konvensional** dalam **mengidentifikasi sindikat fraud** serta kejahatan keuangan yang **terorganisir**.

"Our ability to manufacture fraud now exceeds our ability to detect it." ~ Al Pacino

Frameworks AI/ML (aplikasi teknis)

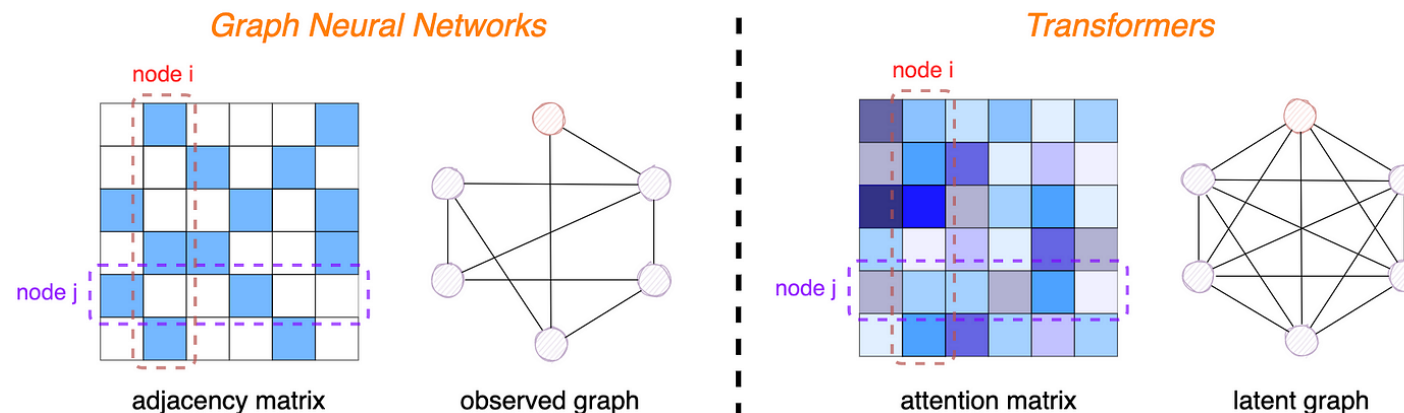
1. GRAPH ANALYTICS

• Nodes & Edges:

- Users (customers dan merchants) bertindak sebagai **nodes**.
- Transactions berlaku sebagai **edges**.

Koneksi ini menciptakan **heterogeneous graph**, dimana nodes dan edges dapat memiliki ciri yang berbeda (user nodes memiliki *account type*, *status*, *device*, dan *demographic attributes*; sedangkan transaction edges memiliki *transaction amount* dan *transaction type*). Menggunakan *Network Analysis*, pengolahan pada data tersebut kemudian dapat dihitung **centrality measures** serta **community detection**-nya.

- **HGT Model (Heterogeneous Graph Transformer):** Metode Graph Neural Network (GNN) ini secara khusus menangani kompleksitas *heterogeneous graph*. Tidak seperti GNN tradisional, **HGT unggul dalam menangkan hubungan antara semua node, terlepas dari keberadaannya transaksinya.**



K-means clustering kemudian digunakan untuk mengelompokkan *cluster groups* yang berperilaku serupa.

Frameworks AI/ML (aplikasi teknis)

2. SUPERVISED LEARNING

- **Data Label:** Kerangka kerja ini menggunakan dua kumpulan data sampel transaksi yang dikategorikan sebagai "Fraud" dan "Non-Fraud".
- **Gradient Boosting Model:** Model ini mampu mengidentifikasi pola dalam data yang mengindikasikan fraud. Setelah ditraining, model dapat menganalisis dataset user dan transaksi baru dan memprediksi kemungkinan bahwa akun tersebut adalah fraud atau bukan.

3. PENDEKATAN FUSI [Graph + Machine-Learning]

HGT mengekstrak fitur dari network. Kemudian, Gradient Boosting menggunakan fitur ini beserta pemahamannya sendiri yang didapat dari training data berlabel untuk menghasilkan parameter sebagai berikut:

- **Syndicate Score:** untuk setiap user relationship, perhitungannya sebagai berikut:

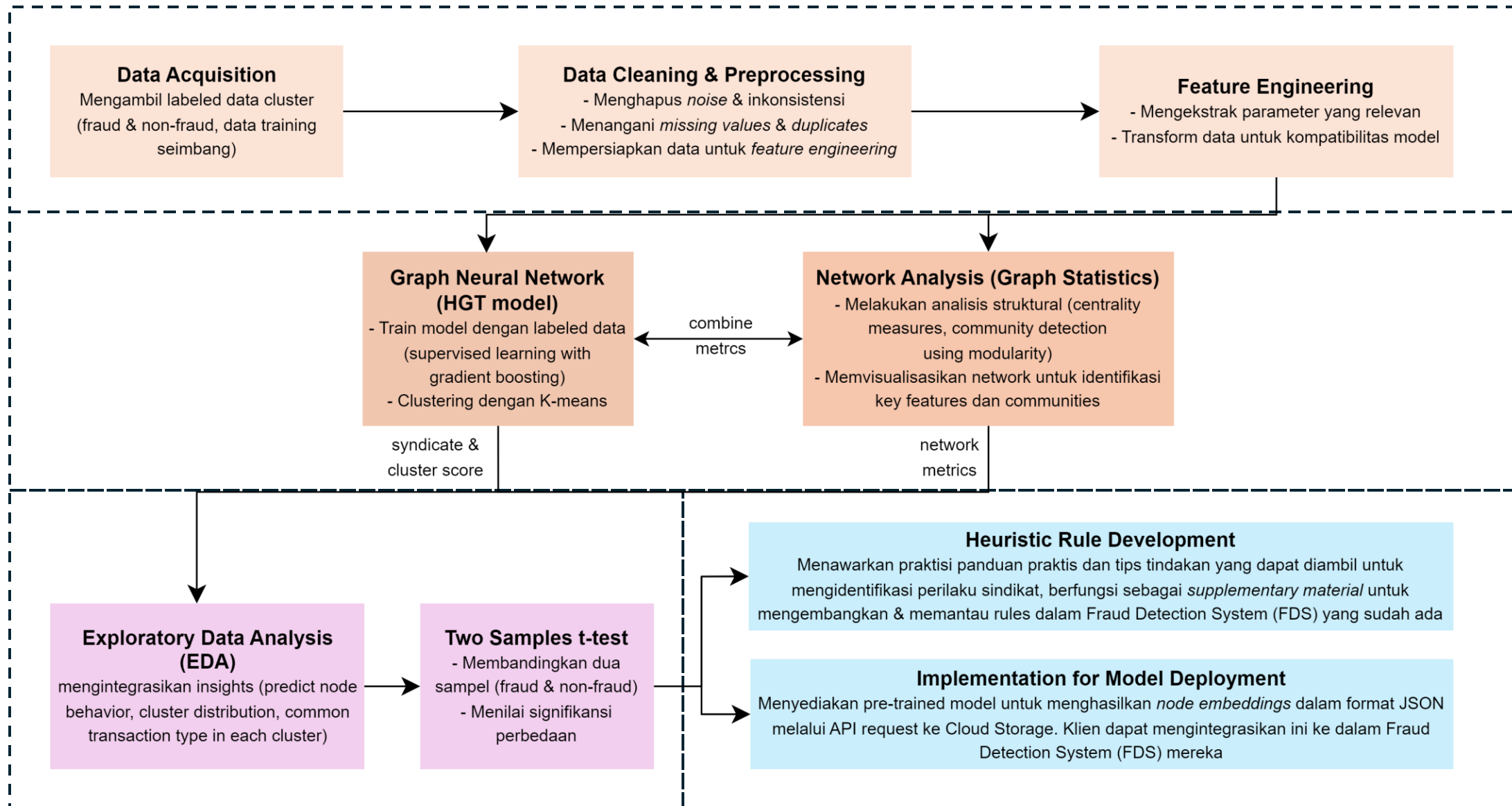
Syndicate Score = $0.4 \times \text{Normalized In-Degree} + 0.4 \times \text{Normalized Out-Degree} + 0.2 \times \text{Normalized Betweenness Centrality}$

- **Cluster Risk Score:** untuk setiap cluster, perhitungannya sebagai berikut:

Risk Level = { "high" if score \geq 67th percentile; "medium" if score $>$ 33rd percentile; "low" otherwise }

By analyzing the four key parameters (**centrality measures, community detection, syndicate score, and cluster risk score**), we can identify potential indicators of fraud syndicates within the network.

AI/ML *Frameworks (pipeline)*



Dataset: Deskripsi dan Struktur

No.	source (v1)	target (v2)	trans amount (v3)	description (v4)
1	*****403- customer	*****195- merchant	1000000	<i>Buy Goods</i>
<i>n</i>

Deskripsi Data:

Data berasal dari transaksi di salah satu PJP *e-wallet* dengan rentang waktu **31 bulan**, sejak Oktober 2021 hingga Mei 2024.

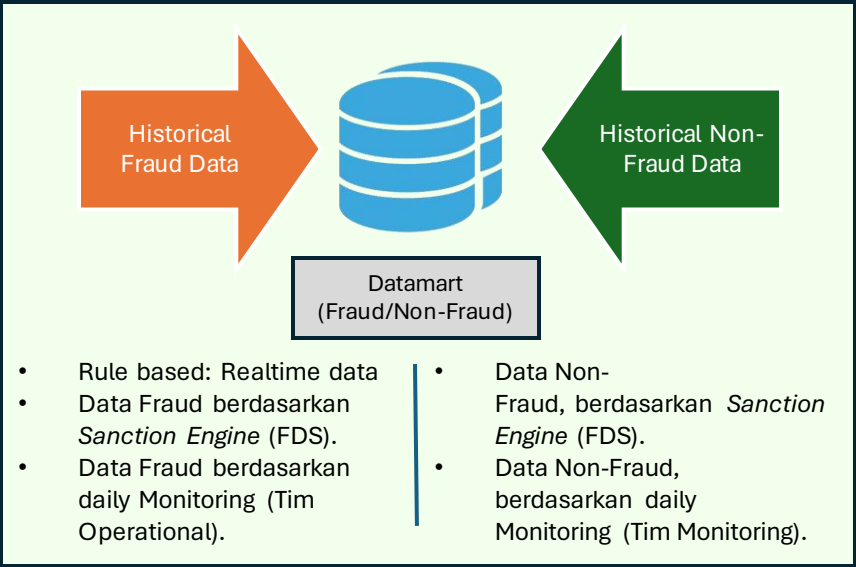
Unsur data format *graph* termasuk; **debit party/sender** (*source node*), **credit party/recipient** (*target node*).

Dataset terbagi dalam dua *sample space* yaitu **‘fraudulent data’ (S1)** dan **‘non-fraudulent data’ (S2)**. Header data termasuk nodes (source & target) dan edges (koneksi & *directionality*[indirected]).

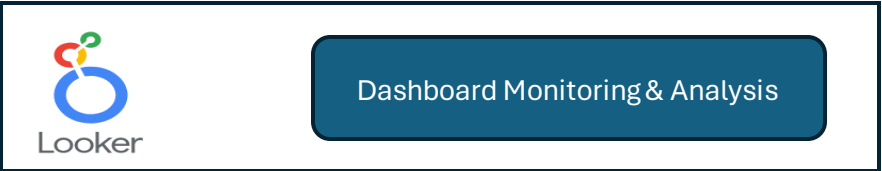
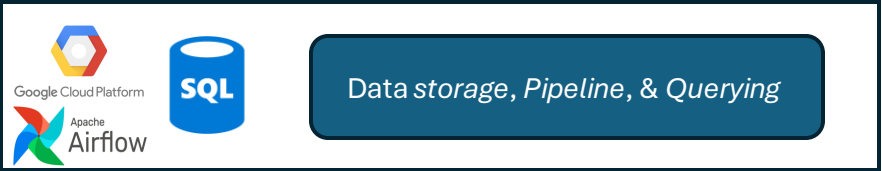
- S1 terdiri dari **2,021,750 edges (1,882,839 transaksi** ke merchant fraud + **138,911 transaksi** dari customer fraud) dan 17,868 nodes (199 merchant fraud; 17,669 customer fraud customer).
- S2 terdiri dari **2,021,750 transaksi (randomized)** dan 113,818 nodes (12,008 merchant, 101,810 customers).

Dataset: Akuisisi dan *Data Quality*

- Akuisisi Data



- Tools **Monitoring & Data Management**



Proses *Data Quality Assurance*

- Data Profiling**
Melakukan analisis data awal untuk memahami struktur, hubungan, dan kualitas data.
- Data *Cleansing***
Mengidentifikasi dan memperbaiki atau menghapus data yang tidak akurat, tidak lengkap, atau tidak konsisten.
- Data *Standardization***
Mengidentifikasi dan memperbaiki atau menghapus data yang tidak akurat, tidak lengkap, atau tidak konsisten.
- Data *Enrichment***
Menambah data dengan informasi tambahan dari sumber eksternal untuk meningkatkan nilainya.
- Regular *Audits***
Melakukan audit berkala untuk memastikan bahwa data tetap berkualitas tinggi dari waktu ke waktu.
- QA Fraud**
Menjaga kualitas dari hasil Analisa baik yang dilakukan secara System dan juga Tim Ops (Manusia) yang berhubungan dengan Fraud melalui adanya pemeriksaan hasil analisa keluaran. Jika diperlukan akan adanya tuning pada parameter rule dan juga coaching untuk pekerja.
- Pelatihan dan penerapan kebijakan**
Melatih staf tentang pentingnya kualitas data dan menerapkan kebijakan yang mendukung praktik pengelolaan data yang baik.



Tools & Teknologi: AI/ML + Pemrosesan Data

- *R programming language*
 - IDE: R-Studio
 - 'stats' package
- *Python programming language*
 - Core Frameworks: TensorFlow, PyTorch, HGTConv, XGBoost
 - Packages tambahan: SciKit-learn (LabelEncoder, KMeans), UMAP, Pandas
 - IDE: Google Colab, Visual Studio Code
- *Gephi graph processing*
- **Apache Airflow**
- **Google Cloud Platform (GCP)**
 - BigQuery *data warehouse*



**AI/ML &
proses
analitikal**



**Statistika
graph &
visualisasi**



***Data
storage,
pipeline, &
querying***

Bisnis Model & Sustainability

KEY PARTNERS

9

- Prinsipal teknologi *Graph Database*
- Provider prinsipal *cloud hosting*
- Regulator dan FIU (PPATK) sebagai *corrector*
- Kementerian/Lembaga;
 - Kementerian Kominfo sebagai *enabler*
 - Dittipidsiber Polri
 - Densus 88/BNPT
 - KPK
 - Ditjen Pajak
 - Bank Indonesia

KEY ACTIVITIES

8

- Penelitian dan pengembangan
- Pemeliharaan sistem
- Pelatihan
- Akuisisi pelanggan
- Kegiatan kepatuhan dan hukum

KEY RESOURCES

7

- Data
- Infrastruktur teknologi
- Sumber Daya Manusia (SDM)
- Paten; kekayaan intelektual (HAKI)

VALUE PROPOSITION

1

- Deteksi, Pencegahan Fraud, dan *Loss Prevention*
- Sekuriti dan perlindungan pengguna
- Implementasi teknis APU-PPT, UU TPPU

CUSTOMER RELATIONSHIP

4

- *Account Manager*
- Asosiasi industry
- Konferensi

CHANNELS

3

- *Online*
- Konferensi
- B2B2G: *Business to Government* atau *Business to Business*
- Penjualan langsung

CUSTOMER SEGMENTS

2

- Industri keuangan non Bank (IKNB), Bank, Penyedia Jasa Pembayaran (PJP), *e-commerce*, Penyedia Infrastruktur Pembayaran
- K/L/O/P (Kementerian, Lembaga, Organisasi Pemerintahan lainnya): Dittipidsiber Polri, Densus 88/BNPT, KPK, Ditjen Pajak

COST STRUCTURE

10

- *Cloud billing*
- Lisensi perangkat lunak dan infrastruktur
- Gaji
- Biaya pemasaran

REVENUE STREAM

5

- *Subscription fee*, atau
- *Usage-based model* (e.g., per API hit)
- *Licensing fee*
- *Implementation & integration fee*
- *Value-added service fee*

ENVIROMENTAL COST

11

- Konsumsi energi
- Limbah Perangkat Keras

SOCIETAL COST

SOCIETAL BENEFITS

6

- Mendukung kepatuhan regulasi
- Meningkatkan kepercayaan pada transaksi digital

ENVIROMENTAL BENEFITS

- Mengurangi jejak karbon
- Alokasi sumber daya yang efisien

Bisnis Model & Sustainability

Value Proposition

- Deteksi, Pencegahan *Fraud*, dan Pencegahan Kerugian untuk memenuhi Peraturan BI No. 23/6/PBI/2021 tentang Penyedia Jasa Pembayaran.
- Keamanan dan perlindungan pengguna untuk memenuhi Peraturan BI No. 3 Tahun 2023 mengenai Perlindungan Konsumen).
- Implementasi teknis APU-PPT (UU No. 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang (UU TPPU)

Customer Segment

- Industri keuangan non Bank (IKNB), Bank, Penyedia Jasa Pembayaran (PJP), *e-commerce*, Penyedia Infrastruktur Pembayaran yang akan dapat disesuaikan dengan kebutuhan masing pelanggan.
- K/L/O/P (Kementerian, Lembaga, Organisasi Pemerintahan lainnya) : Dittipidsiber Polri, Densus 88/BNPT, KPK, Ditjen Pajak

Channels

- *Online*, melalui *web-site*, *mailing list*, *online meeting*.
- Konferensi yang diadakan oleh regulator dan/atau asosiasi industri dan konferensi yang bersifat
- B2B2G: *Business to Government* atau *Business to Business*
- Penjualan langsung melalui kunjungan ke pelanggan potensial.

Customer Relationship

- *Account Manager* sebagai pihak bertanggung jawab atas hubungan antara perusahaan tersebut dengan pelanggan atau klien .
- Asosiasi untuk menjalin hubungan dengan pelaku industri termasuk, Asosiasi Sistem Pembayaran Indonesia (ASPI).

Revenue Stream

- *Subscription fee*, per-bulan ataupun per-tahun sesuai kebutuhan pelanggan, atau
- *Usage-based model*, *fee* yang dikenakan setiap penggunaan atau permintaan terhadap sebuah layanan API (*per API hit*) atau setiap *customer ID* tersedia (*per CIF ID registered*)
- *Implementation and integration fee*, biaya dikenakan untuk mengatur dan mempersiapkan suatu produk atau layanan untuk digunakan oleh pelanggan.
- *Value-added service fee*, mencakup biaya personalisasi sesuai kebutuhan pelanggan.

Societal Benefits / Environmental Benefits

- Mendukung kepatuhan regulasi, seperti Undang-Undang terkait Anti Pencucian Uang (AML) dari PPATK, peraturan Bank Indonesia (BI), dan Otoritas Jasa Keuangan (OJK).
- Meningkatkan kepercayaan pada transaksi digital, termasuk mendapatkan kepercayaan konsumen dan kepercayaan bisnis.
- Mengurangi jejak karbon. Pengurangan penggunaan *hardware* & penempatan server di lokasi *Eco-Green* dengan sumber daya listrik terbaru
- Alokasi sumber daya yang efisien, mengurangi penggunaan sumber daya yang signifikan, termasuk perjalanan, kertas, dan bahan lainnya.

VALUE PROPOSITION

1

- Deteksi, Pencegahan *Fraud*, dan Pencegahan Kerugian
- Sekuriti dan perlindungan pengguna
- Implementasi teknis APU-PPT, UU TPPU

CUSTOMER RELATIONSHIP

4

- *Account Manager*
- Asosiasi industri
- Konferensi

CHANNELS

3

- Online
- Konferensi
- B2B2G: *Business to Government* atau *Business to Business*
- Penjualan langsung

CUSTOMER SEGMENTS

2

- Industri keuangan non Bank (IKNB), Bank, Penyedia Jasa Pembayaran (PJP), *e-commerce*, Penyedia Infrastruktur Pembayaran
- K/L/O/P (Kementerian, Lembaga, Organisasi Pemerintahan lainnya) : Dittipidsiber Polri, Densus 88/BNPT, KPK, Ditjen Pajak

REVENUE STREAM

5

- *Subscription fee*
- *Usage-based model (e.g., per API hit)*
- *Licensing fee*
- *Implementation & integration fee*
- *Value-added service fee*

SOCIETAL BENEFITS

/

ENVIROMENTAL BENEFITS

6

- Mendukung kepatuhan regulasi
- Meningkatkan kepercayaan pada transaksi digital
- Mengurangi jejak karbon
- Alokasi sumber daya yang efisien

KEY PARTNERS

9

- Prinsipal teknologi *Graph Database*
- Provider prinsipan *cloud hosting*
- Regulator dan FIU (PPATK) sebagai *corrector*
- K/L/O/P;
 - Kementerian Kominfo sebagai *enabler*
 - Dittipidsiber Polri
 - Densus 88/BNPT
 - KPK
 - Ditjen Pajak
 - Bank Indonesia

KEY ACTIVITIES

8

- Penelitian dan pengembangan
- Pemeliharaan sistem
- Pelatihan
- Akuisisi pelanggan
- Kegiatan kepatuhan dan hukum

KEY RESOURCES

7

- Data
- Infrastruktur teknologi
- Sumber Daya Manusia (SDM)
- Paten; kekayaan intelektual (HAKI)

Key Resources

- Data yang digunakan untuk dijadikan rules pada Fraud Detection System
- Infrastruktur Teknologi, termasuk perangkat lunak untuk Bahasa pemograman R & Python, *graph processing*, dan cloud.
- Sumber Daya Manusia meliputi; Data Engineer, AI/ML Engineer, API Developer, *Fraud Operations/tactical monitoring, investigator fraud.*
- Paten; kekayaan intelektual (HAKI)

Key Activities

- Penelitian dan pengembangan termasuk akuisisi data, pembersihan dan pengolahan ulang data, rekayasa fitur, pemodelan, analisis struktural, eksplorasi data, melakukan uji-t, pengembangan dan implementasi.
- Pemeliharaan sistem, dilakukan berkala termasuk untuk produk yang digunakan oleh Pelanggan.
- Pelatihan yang diadakan untuk Pelanggan yang menggunakan produk.
- Akuisisi pelanggan
- Kegiatan Kepatuhan & Hukum

Key Partners

- Prinsipal teknologi *Graph Database*
- Provider prinsipan *cloud hosting*
- Regulator dan FIU (PPATK) sebagai *corrector*
- Kementerian /Lembaga/Organisasi /Perangkat Daerah untuk menambahkan *source data*, seperti;
 - Kementerian Kominfo sebagai *enabler*
 - Dittipidsiber Polri seperti Daftar Pencarian Orang (DPO)
 - Densus 88/BNPT
 - KPK
 - Ditjen Pajak
 - Bank Indonesia, seperti daftar hitam nasional

COST STRUCTURE

10

- *Cloud billing*
- Lisensi perangkat lunak dan infrastruktur
- Gaji
- Biaya pemasaran

ENVIROMENTAL COST

/

SOCIETAL COST

11

- Konsumsi energi
- Limbah Perangkat Keras

Cost Structure

- *Cloud billing* untuk penyimpanan data
- Lisensi Perangkat Lunak & Infrastruktur
- Gaji
- Biaya Pemasaran termasuk biaya untuk mengadakan konferensi, *website* dan kunjungan langsung ke Pelanggan (jika dibutuhkan)

Environmental Cost / Societal Cost

- Konsumsi Energi, termasuk listrik.
- Limbah Perangkat Keras yang timbul dari perangkat keras yang sudah tidak dapat digunakan.

Rancangan **Prototype**: *Heuristic Rule Development*

- Deliverables*: Kerangka pemodelan berbasis graph & AI/ML yang mampu membedakan dan mendeteksi jaringan fraud dan non-fraud.



Observed Fraud Syndicate



Observed Network of Non-Fraudulent Nodes

Table 4. Fraud syndicate and cluster score

No.	HGT cluster	syndicate score	cluster risk score	cluster risk level	node count
1.	0	0.12	0.15	Low	2563
2.	1	0.54	0.67	Medium	11987
3.	2	0.76	0.82	Medium	553
4.	3	0.93	0.97	High	625

Table 5. Non-Fraud syndicate and cluster score

No.	HGT cluster	syndicate score	cluster risk score	cluster risk level	node count
1.	0	0.05	0.02	Low	10233
2.	1	0.15	0.10	Low	89795
3.	2	0.21	0.20	Low	11783
4.	3	0.32	0.35	Medium	3007

Table 6. Comparison between fraud and non-fraud clusters

Cluster	Fraud Syndicate Analysis	Non-Fraud Syndicate Analysis
0	Lowest activity, Syndicate Score: 0.12, minimal degree and betweenness centralities, peripheral with insignificant risk.	Mostly inactive nodes, Syndicate Score: 0.05, minimal centrality, low node engagement, negligible risk.
1	Largest cluster, Syndicate Score: 0.54, low degree centrality, medium risk.	Holds bulk of nodes, Syndicate Score: 0.15, sparse interactions, typical of regular customers, low risk.
2	Higher risk, Syndicate Score: 0.76, higher transaction volume, limited external influence.	Slightly more frequent transactions, Syndicate Score: 0.21, somewhat higher centrality, low risk.
3	Highest risk, Syndicate Score: 0.93, significant network centrality, core role in fraud activities.	Most active in legitimate scenarios, Syndicate Score: 0.32, central role in transactions, medium risk level.

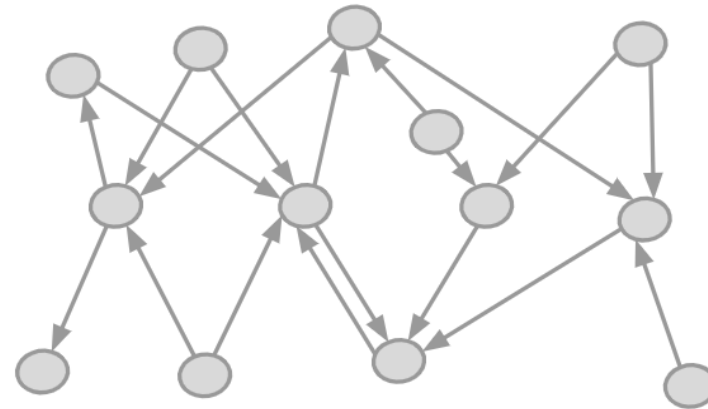
Rancangan **Prototype: *Deployment Model***

- Delivery: PyTorch model (.pth), python script (.py) for creating node embeddings* with the HGT model

Example Input (the input from CSV table format)

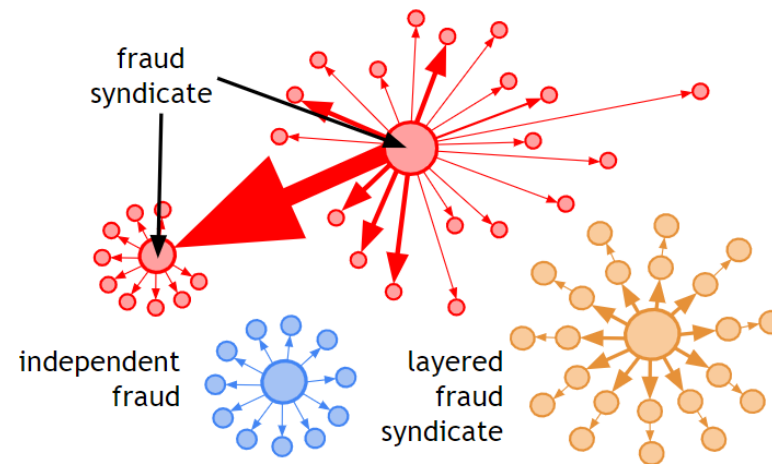
```
def load_data_and_process(project_id):
    print(elapsed(), "running query...")
    df = query(project_id)
    # df = pd.read_csv("./gnn_fraud_sampling.csv")
    print(elapsed(), "finished running query")
```

	source_node	target_node	trans_amount	attributes
0	015-merchant	223-merchant	89500	
1	015-merchant	689-merchant	499380	
2	015-merchant	894-merchant	4243	
3	015-merchant	286-merchant	300000	



Example Result (the output from HGT model processing → will be stored in JSON format in Cloud Storage)

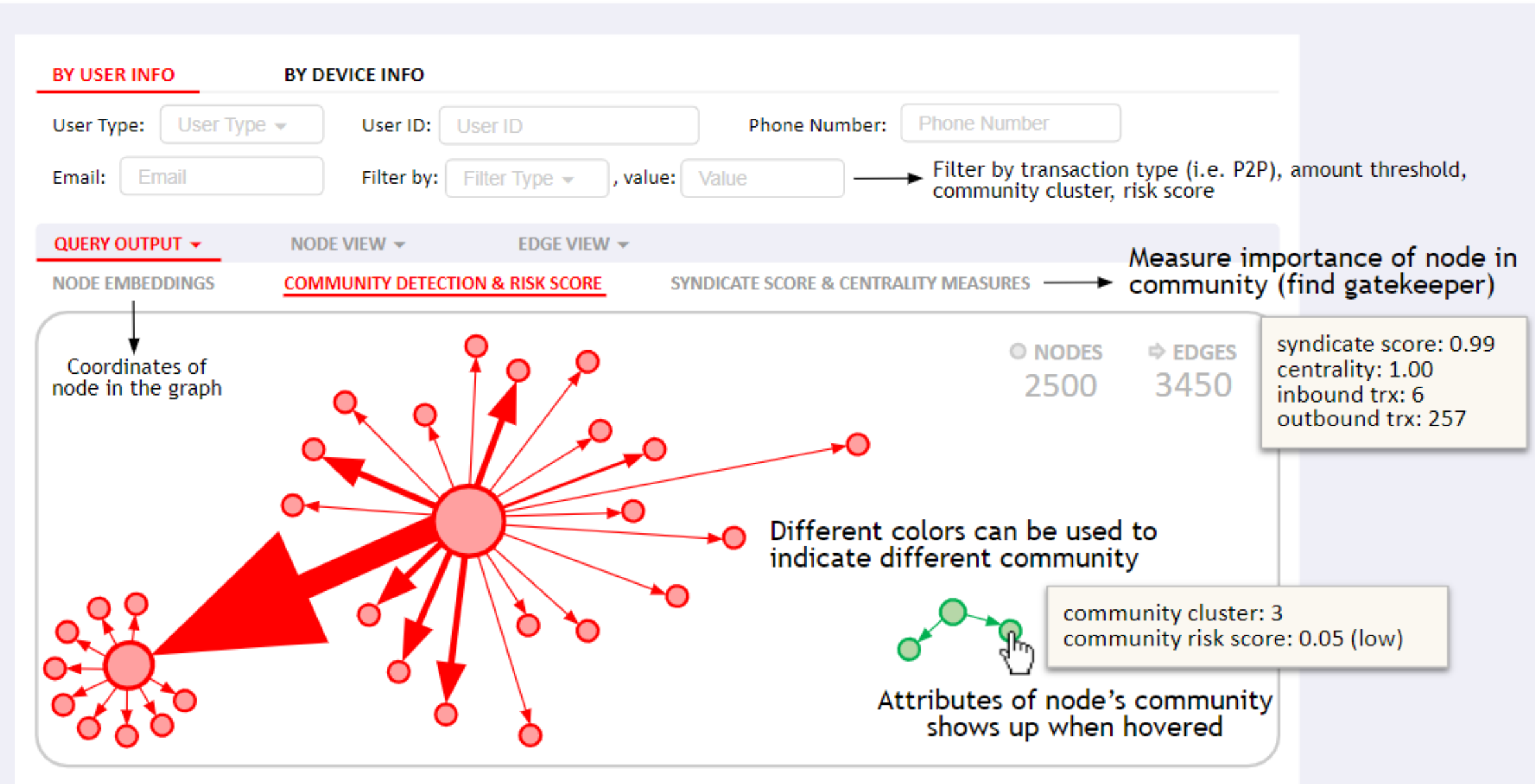
```
{
  "_id": ObjectId("..."), // Unique identifier
  "user_id": 12345678, // Node ID
  "type": "user", // Node type (e.g., user or transaction)
  "attributes": { // Other relevant node data (optional)
    "parameter_1": "xxxxx",
    "parameter_2": "xxxxx",
    ...
    "parameter_n": "xxxxx",
  },
  "embedding": [0.234, 0.567, -0.123]
  // HGT node embedding as a list of numbers (coordinates)
}
```



from this
to this

*node embeddings = vector representations/node's position in the graph, used to plot graph network visualization

Mockup: Possible Implementation in Fraud Detection System (FDS)



Penutup

Tata kelola perusahaan yang baik tidak hanya tentang kestabilan moneter dan pemanfaatan teknologi, tetapi juga tentang komitmen terhadap ESG dan digitalisasi yang **terintegrasi**. **Kepercayaan masyarakat** dan **perlindungan konsumen** adalah fondasi dari masa depan yang **berkelanjutan** dan **inovatif**.

"Fraudsters collaborate, why shouldn't you?"

~ GNERATE, Fraud Detection System

Referensi

- Europol. (2023). Online Fraud Schemes: A Web Of Deceit. Internet Organised Crime Threat Assessment (IOCTA). European Cybercrime Centre (EC3). Link: <https://www.europol.europa.eu/publications-events/main-reports/iocta-report>
- FATF – Interpol - Egmont Group. (2023). Illicit Financial Flows from Cyber-Enabled Fraud, FATF, Paris, France. Link: <http://fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/illicit-financial-flows-cyberenabled-fraud.html>
- He, E., Hao, Y., Zhang, Y., Yin, G., & Yao, L. (2024). SCALA: Sparsification-based Contrastive Learning for Anomaly Detection on Attributed Networks. arXiv preprint arXiv:2401.01625.
- World Bank. (2021). Press Release: “COVID-19 Drives Global Surge in use of Digital Payments”. The Global Findex Database 2021: Financial Inclusion, Digital Payments, and Resilience in the Age of COVID-19. <https://www.worldbank.org/en/news/press-release/2022/06/29/covid-19-drives-global-surge-in-use-of-digital-payments>
- Kemenko Perekonomian. (2024). Menko Airlangga: Digitalisasi Menjadi Salah Satu Andalan Mesin Pertumbuhan Ekonomi Baru Bagi Ketahanan Ekonomi Mendatang. *Kementerian Koordinator Bidang Perekonomian Republik Indonesia siaran Pers*. Link: <https://www.ekon.go.id/publikasi/detail/5639/menko-airlangga-digitalisasi-menjadi-salah-satu-andalan-mesin-pertumbuhan-ekonomi-baru-bagi-ketahanan-ekonomi-mendatang>

Lampiran

GitHub repository:

<https://github.com/natgluons/Syndicate-Indication-using-Network-Graph-Analytics>