

FraudVis: Understanding Unsupervised Fraud Detection Algorithms

Jiao Sun[1], Qixin Zhu[1], Zhifei Liu[1], Xin Liu[1], Jihae Lee[1], Lei Shi[2], Zhigang Su[3], Ling Huang[1] and Wei Xu[1]

[1] Institute of Interdisciplinary Information Sciences, Tsinghua University
[2] SKLCS, Institute of Software, Chinese Academy of Sciences
[3] JD.com

Motivation

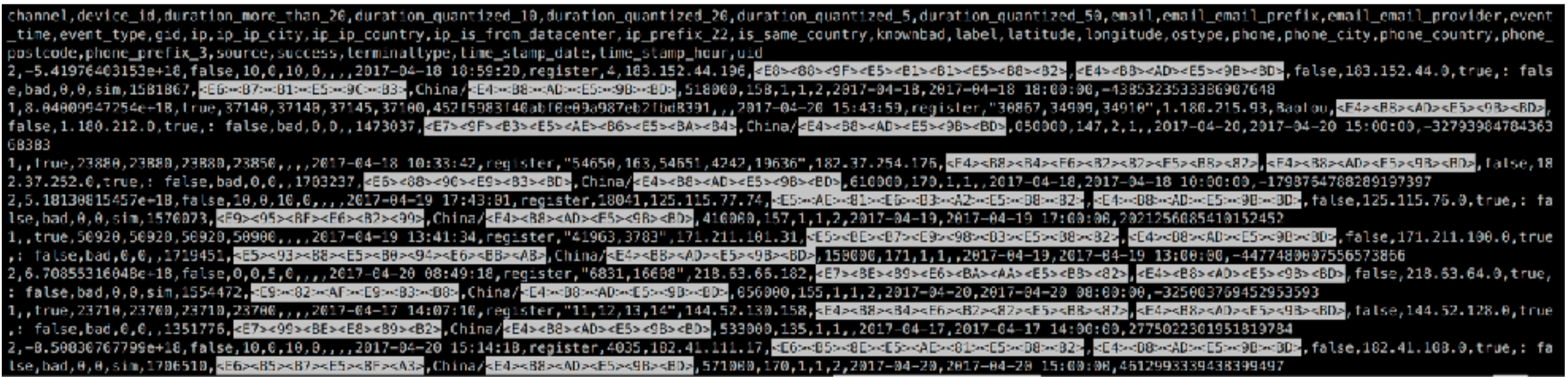
- Great loss caused by fraud users
  - Various kinds of fraud behavior
- Difficulty in distinguishing fraud users from normal users
  - Camouflage in **individuals**
  - **Collaborative** behavior
- Algorithm itself is hard to interpret
  - Feature selection is a black-box to user
  - The origin of “group” and why a group is abnormal

What are fraudsters?

		ostype	ip_prefix_22	phone_city	phone_prefix_3	duration_quantized_20	label	id
30	good	android	101.90.252.0	上海	180	0	good	30
40	good	sim	114.95.156.0	上海	131	0	good	40
55	good	android	101.229.16.0	上海	137	0	good	55
63	good	android	1.197.176.0	上海	138	0	good	63
200	good	sim	117.136.8.0	上海	134	0	good	200
299	good	android	180.172.168.0	上海	156	0	good	299
458	bad	android	113.122.4.0	上海	170	0	bad	458
474	bad	android	119.122.96.0	上海	170	0	bad	474
491	bad	android	58.54.220.0	上海	170	0	bad	491
498	bad	android	117.66.192.0	上海	170	0	bad	498
519	bad	android	114.106.224.0	上海	170	0	bad	519
529	bad	android	112.113.60.0	上海	170	0	bad	529
531	bad	android	59.53.140.0	上海	170	0	bad	531
540	bad	android	27.27.172.0	上海	170	0	bad	540
544	bad	android	123.161.152.0	上海	170	0	bad	544
572	bad	android	114.239.0.0	上海	170	0	bad	572
614	bad	android	117.81.116.0	上海	170	0	bad	614
626	bad	android	120.32.128.0	上海	170	0	bad	626
639	bad	android	180.124.44.0	上海	170	0	bad	639
650	bad	android	117.93.140.0	上海	170	0	bad	650
652	bad	android	220.179.212.0	上海	170	0	bad	652
677	bad	android	180.122.20.0	上海	170	0	bad	677

Challenges

- High-dimensional datasets
  - Various kinds of fraud behavior
  - High-dimensional data for each log
- Selection of features and algorithms
  - Hard to evaluate which ones are useful
  - Heavily depends on the scenario
- No labels
  - No label for evaluation
  - High cost for false positive



Works for both algorithm experts and domain experts

- Why do users belong to the same group?
- What are the important features?
- What did they do as a fraud group?
- Do they have some correlations?
- Is the user good or not?

domain experts

- What causes the form of a fraud group?
- What are the distributions of the important features?
- Do users in the same group share the same pattern?
- Will members in one group build a strange network?
- Did I make a mistake for this user?

algorithm experts

Works for both algorithm experts and domain experts

- Why do users belong to the same group?
- **What are the important features?**
- What did they do as a fraud group?
- Do they have some correlations?
- Is the user good or not?

domain experts

- What causes the form of a fraud group?
- **What are the distributions of the important features?**
- Do users in the same group share the same pattern?
- Will members in one group build a strange network?
- Did I make a mistake for this user?

algorithm experts

Works for both algorithm experts and domain experts

- Why do users belong to the same group?
- **What are the important features?**
- What did they do as a fraud group?
- **Do they have some correlations?**
- Is the user good or not?

domain experts

- What causes the form of a fraud group?
- **What are the distributions of the important features?**
- Do users in the same group share the same pattern?
- **Will members in one group build a strange network?**
- Did I make a mistake for this user?

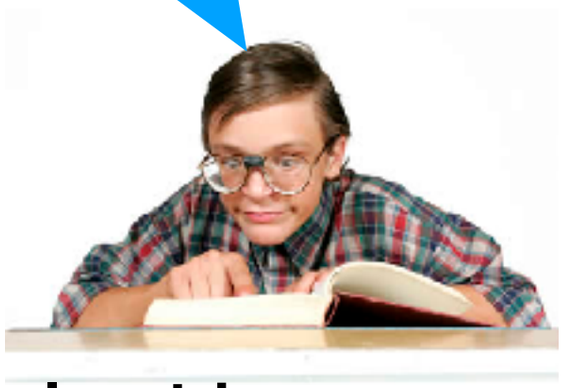
algorithm experts

Works for both algorithm experts and domain experts

- Why do users belong to the same group?
- **What are the important features?**
- What did they do as a fraud group?
- **Do they have some correlations?**
- **Is the user good or not?**

domain experts

- What causes the form of a fraud group?
- **What are the distributions of the important features?**
- Do users in the same group share the same pattern?
- **Will members in one group build a strange network?**
- **Did I make a mistake for this user?**



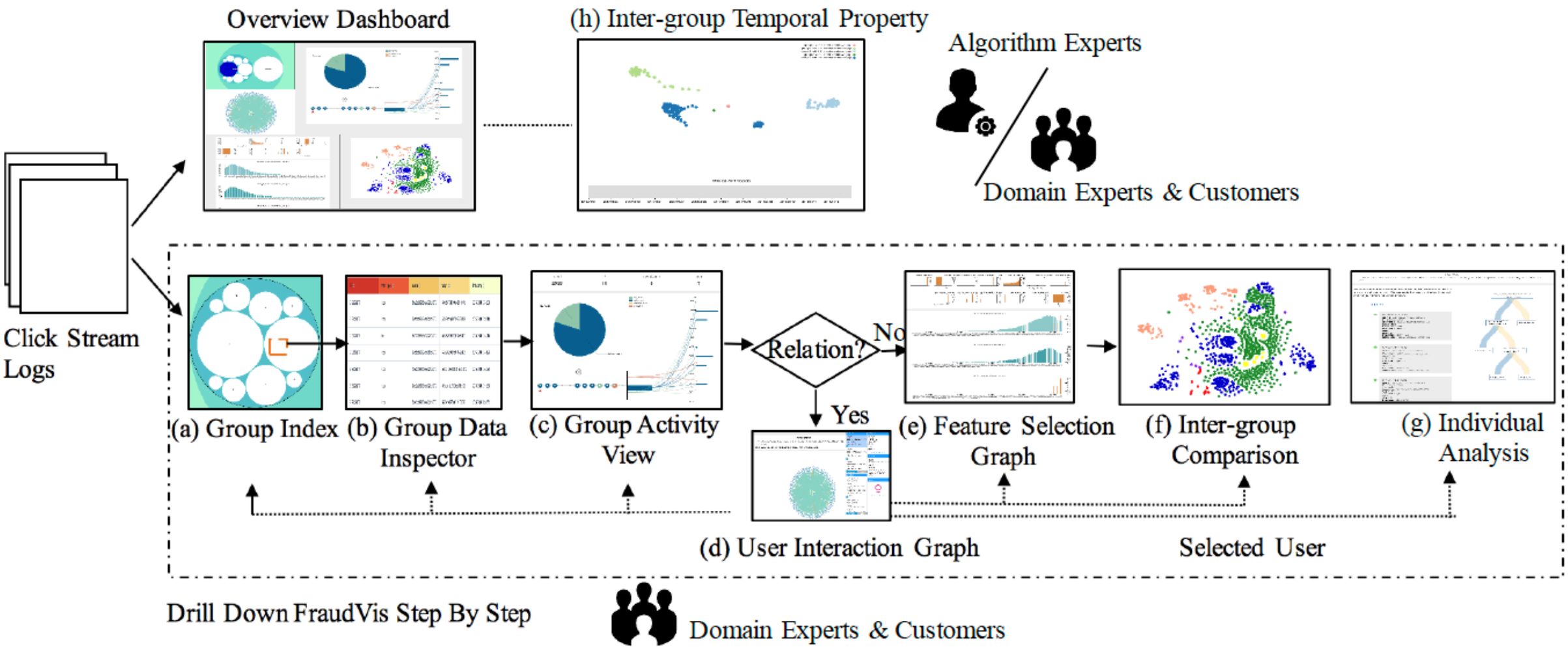
algorithm experts

We need VISUALIZATION!

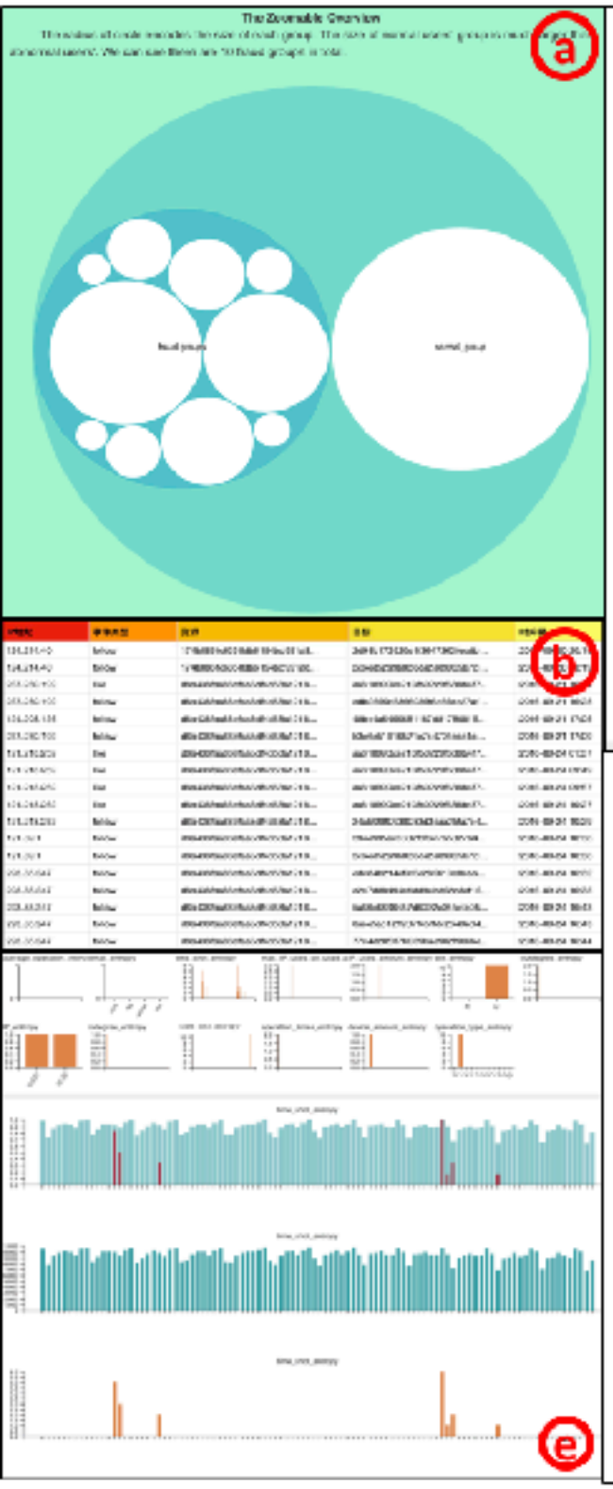
Main contributions

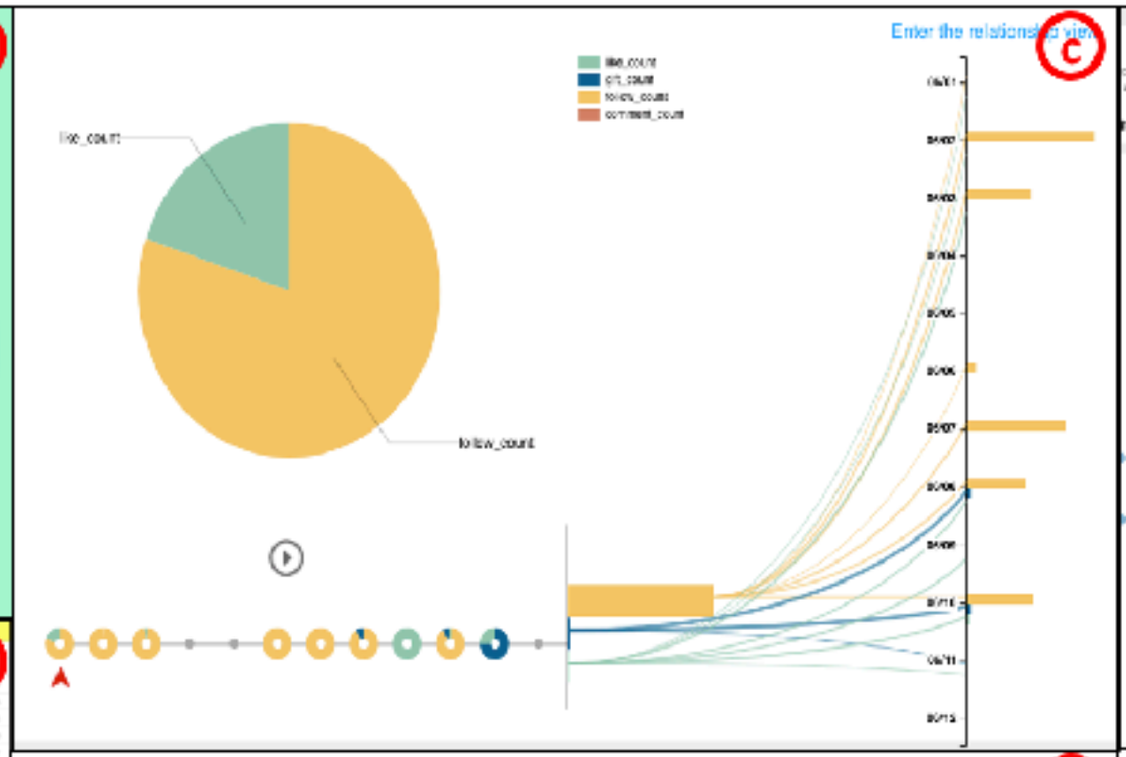
- Comprehensive analysis
  - Inter-group, intra-group, individual
  - Correlation, temporal, spatial
- Visualization interpretation of algorithm result through customized interactions
  - Instructions
  - Different dashboards
- Evaluation through real-world data sets and algorithms

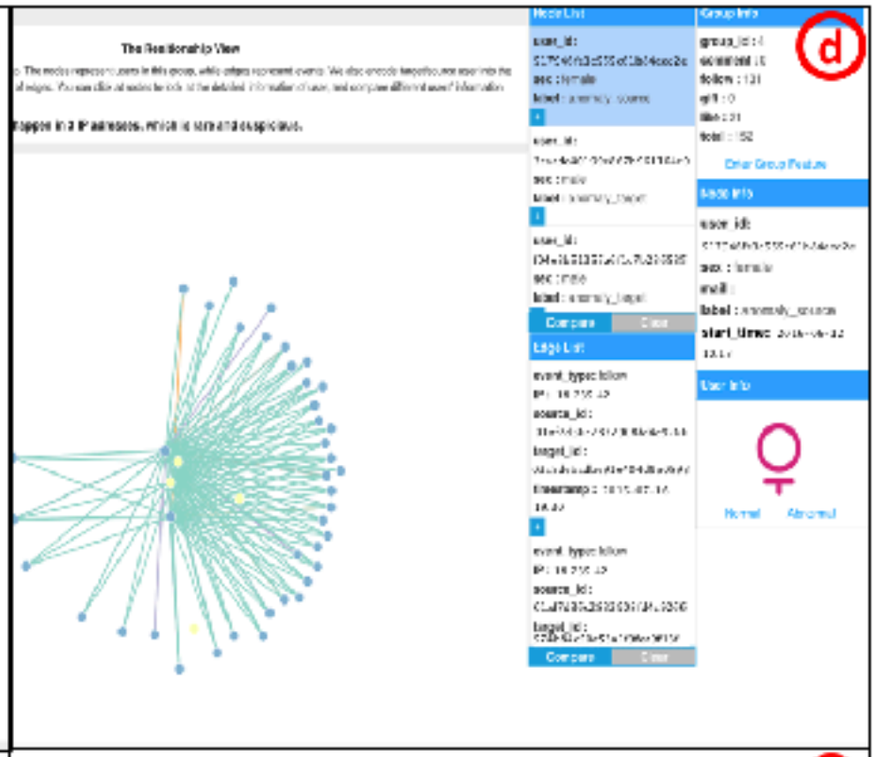
Workflow

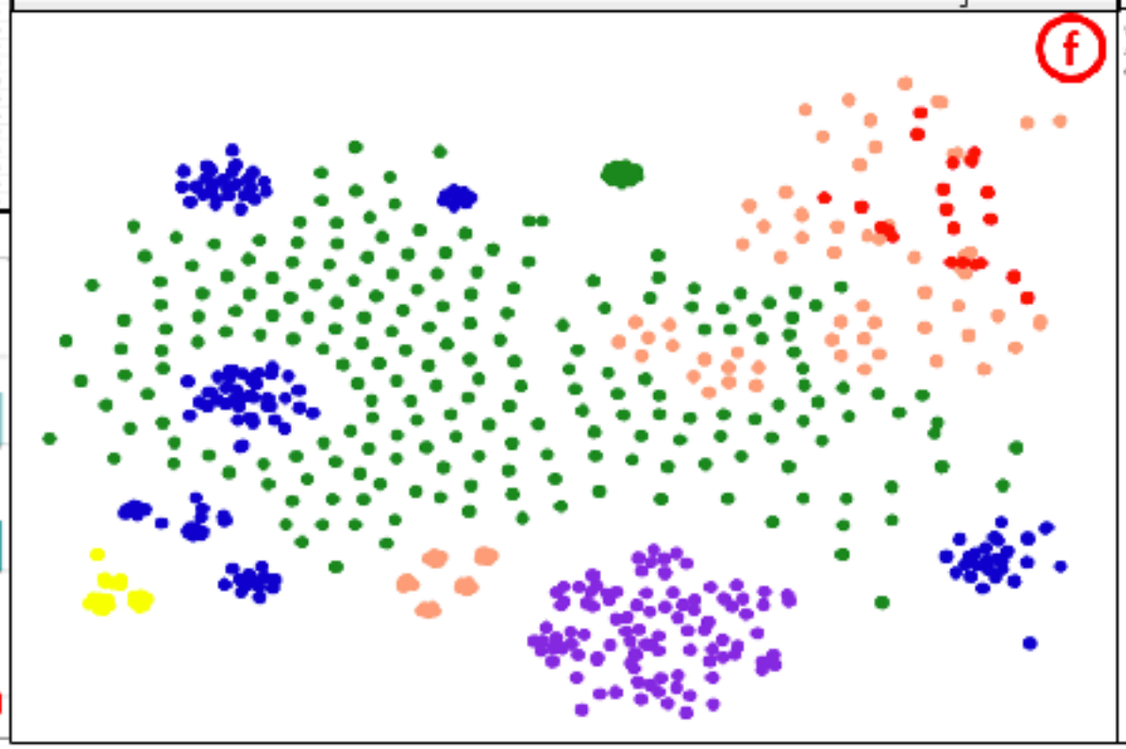

Overview Dashboard
(h) Inter-group Temporal Property
Algorithm Experts
Domain Experts & Customers
Click Stream Logs
(a) Group Index
(b) Group Data Inspector
(c) Group Activity View
Relation?
No
Yes
(e) Feature Selection Graph
(f) Inter-group Comparison
(g) Individual Analysis
(d) User Interaction Graph
Selected User
Drill Down FraudVis Step By Step
Domain Experts & Customers

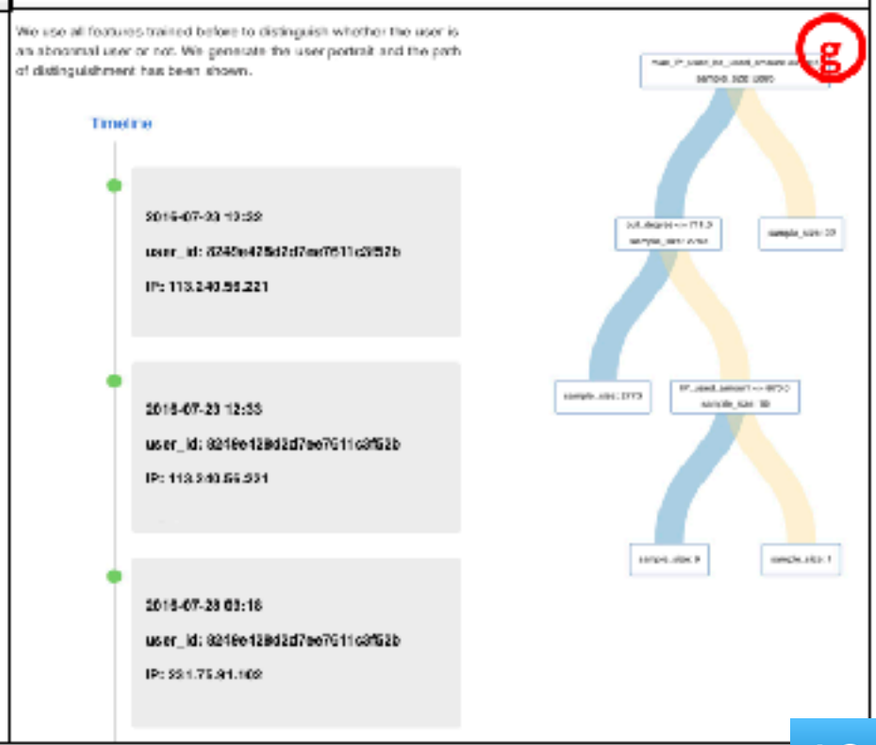
Overview Dashboard



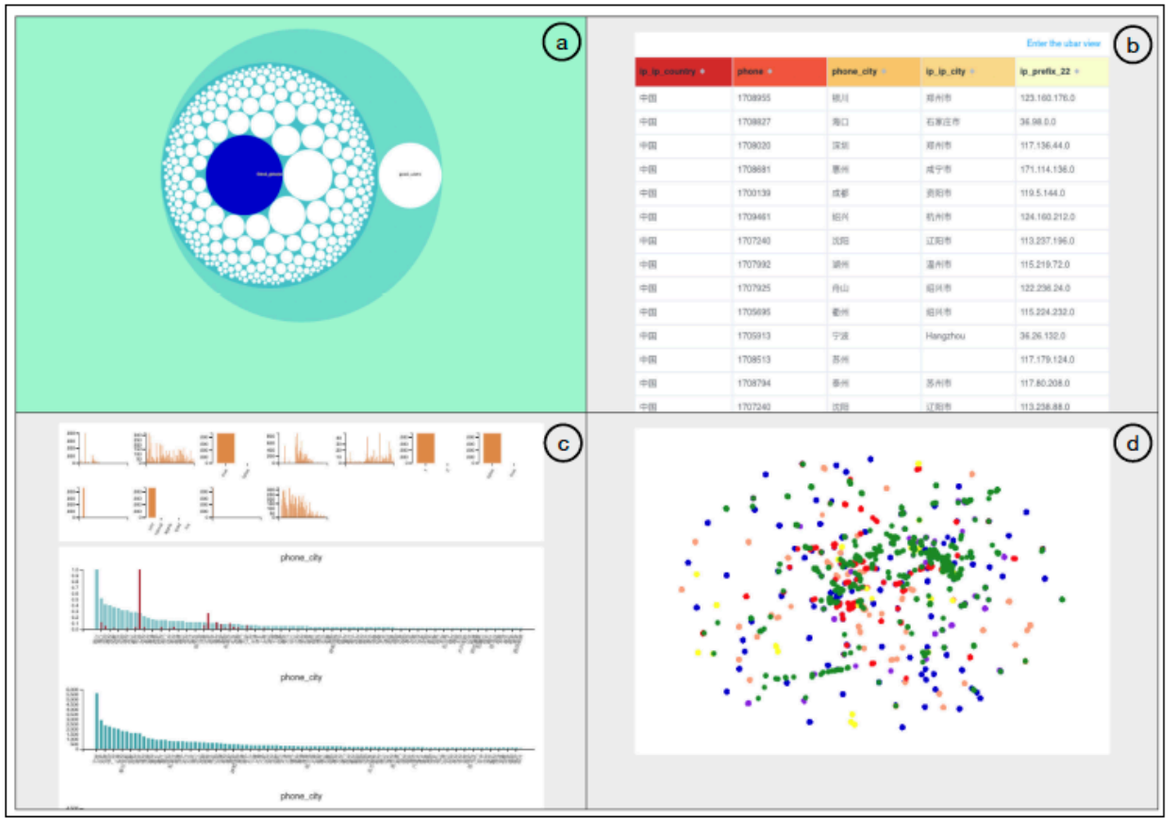




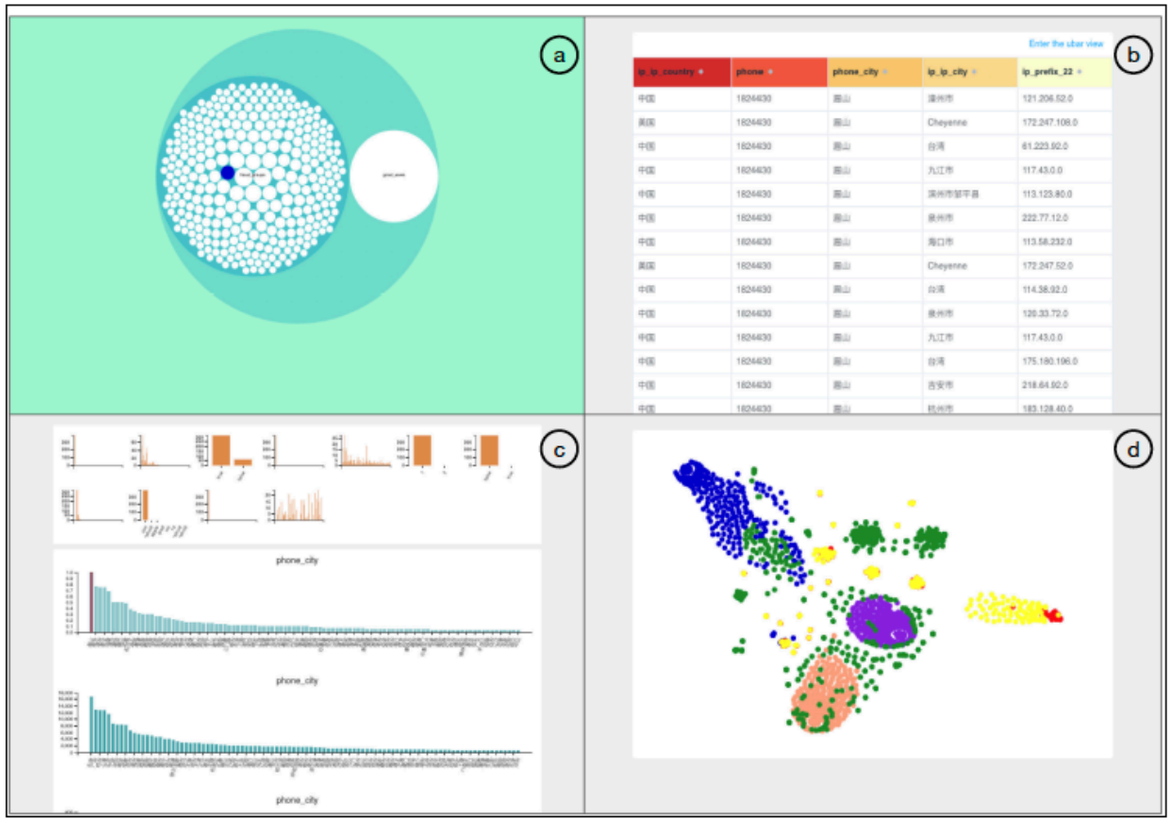




Case study 2: E-commerce Website



(a) stock k-means



(b) improved

- The distribution of the most important feature hardly differ from the overall distribution
- Members from different groups are mixed together and hard to separate
- Large fraud group containing many users that are not similar

Conclusion

- We solve two main problems
  - How to explain the fraud behavior to domain users with little technology background?
  - How to test the result of various fraud detection algorithms and discover the fundamental features?
- A fresh view and a working system to display high-dimensional fraud behaviors
- Visually interpret and compare the result of unsupervised fraud detection algorithms

The future of Fraud Detection

Good detection algorithms

+

VISULIZATION

Thanks & QA

Jiao Sun - https://sunjiao123sun.github.io
Email: j-sun16@mails.tsinghua.edu.cn

All kinds of collaboration are welcomed! 😄