LAC : LSTM AUTOENCODER with Community for Insider Threat Detection

Sudipta Paul[1,2] Subhankar Mishra[1,2]

[1]National Institute of Science, Education and Research Bhubaneswar, Odisha, India-752050
[2]Homi Bhaba National Institute, Anushaktinagar, Mumbai, India-400094

Presented by
Sudipta Paul
sudiptapaulvixx@niser.ac.in

Outline

- Introduction
- Insider Threat Detection
- Autoencoder
- LSTM
- LSTM Autoencoder
- Community Detection
- LAC: LSTM AUTOENCODER with Community for Insider Threat Detection
- Future Direction
- Conclusion

Introduction I

- **Insiders** are persons within the organizations trusted with sensitive and personal information.
- **Insider threat detection**[1][2] is the process of finding out potential threats through their *unauthorized actions* leading to damage to the organizations such as data leaks.
- These *unauthorized actions* can be found out with the help of the network data analysis of that organization.

---

[1] Aram Kim et al. "A Review of Insider Threat Detection Approaches With IoT Perspective". In: *IEEE Access* 8 (2020), pp. 78847–78867.

[2] Robin Sommer and Vern Paxson. "Outside the closed world: On using machine learning for network intrusion detection". In: *2010 IEEE symposium on security and privacy*. IEEE. 2010, pp. 305–316.

Introduction II

- In general the main inspiration behind this type of analysis is to find the *Outlier*[3] in the network data and whether it is *Anomaly*[4] or not.
- A psychology and social studies topic "**Group Dynamics**"[5] defines the affect of "group" on individual. We took this in account and applied this in our approach in a novel way.

[3] Charu C Aggarwal. "Outlier analysis". In: *Data mining*. Springer. 2015, pp. 237–263.

[4] Varun Chandola, Arindam Banerjee, and Vipin Kumar. "Anomaly detection for discrete sequences: A survey". In: *IEEE Transactions on Knowledge and Data Engineering* 24.5 (2010), pp. 823–839.

[5] Donelson R Forsyth. *Group dynamics*. Cengage Learning, 2018.

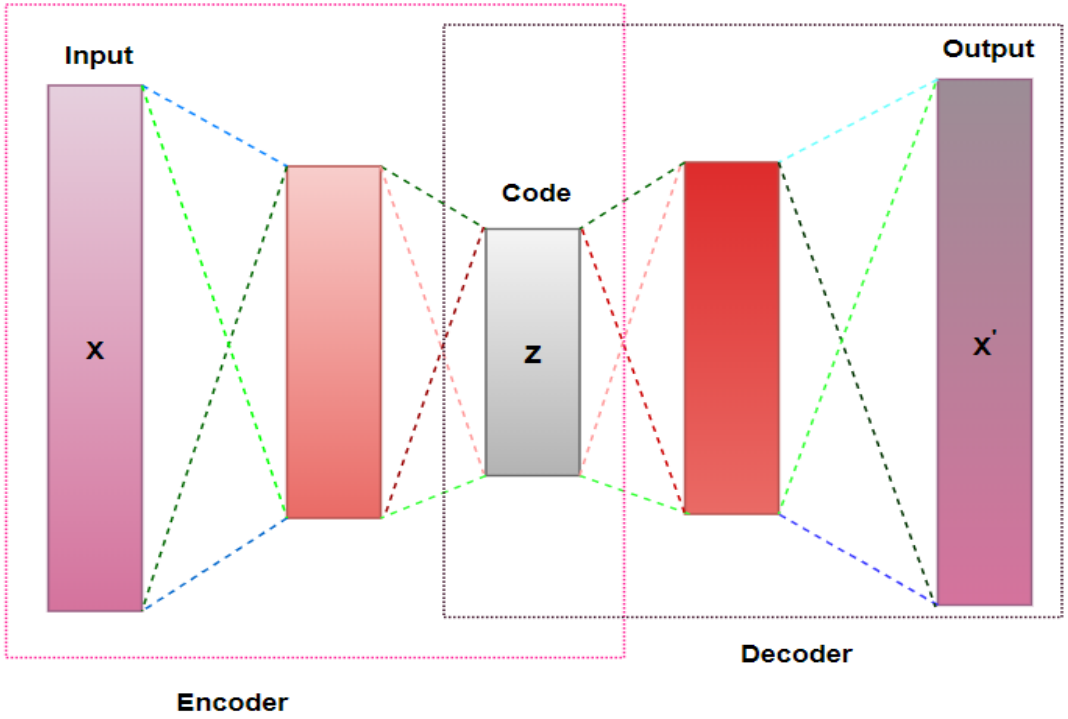
Insider Threat Detection

- The employees of any organization, institute or industry, spend a significant amount of time on computer network, where they develop their own routine of activities in the form of network transactions over a time period.
- **Insider threat detection**[6] involves identifying deviations in the routines or anomalies which may cause harm to the organization in the form of data leaks and secrets sharing.
- **Anomaly** can be defined as an outlier in a set of dataset which affects the entirety in an unacceptable way.
- An **outlier**[7] is "an observation which deviates so much from other observations as to arouse suspicions that it was generated by a different mechanism".

[6] Fangfang Yuan et al. "Insider threat detection with deep neural network". In: *International Conference on Computational Science*. Springer. 2018, pp. 43–54.

[7] Douglas M Hawkins. *Identification of outliers*. Vol. 11. Springer, 1980.

Autoencoder

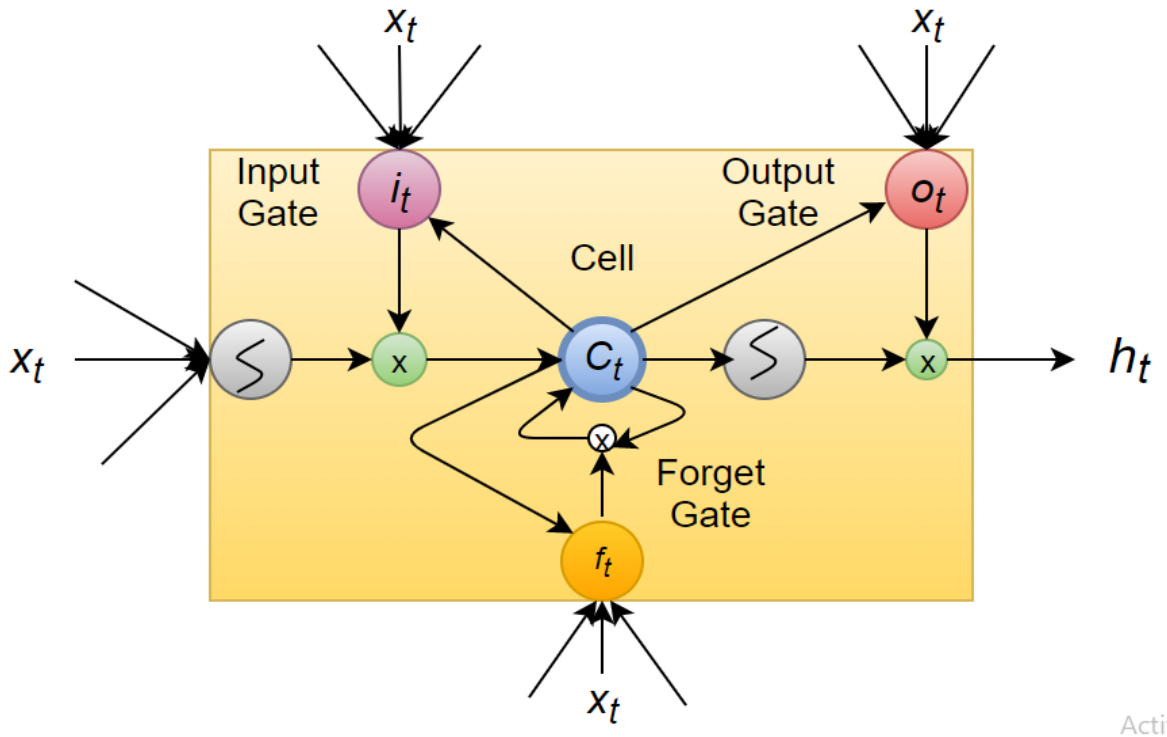


- An Autoencoder[8][9] is an unsupervised neural network.
- It is restricted in a certain manner which forces it to copy approximately, somehow similar to the input training data.

[8] Ian Goodfellow, Yoshua Bengio, and Aaron Courville. *Deep learning*. MIT press, 2016.

[9] Jinwon An and Sungzoon Cho. "Variational autoencoder based anomaly detection using reconstruction probability". In: *Special Lecture on IE* 2.1 (2015).

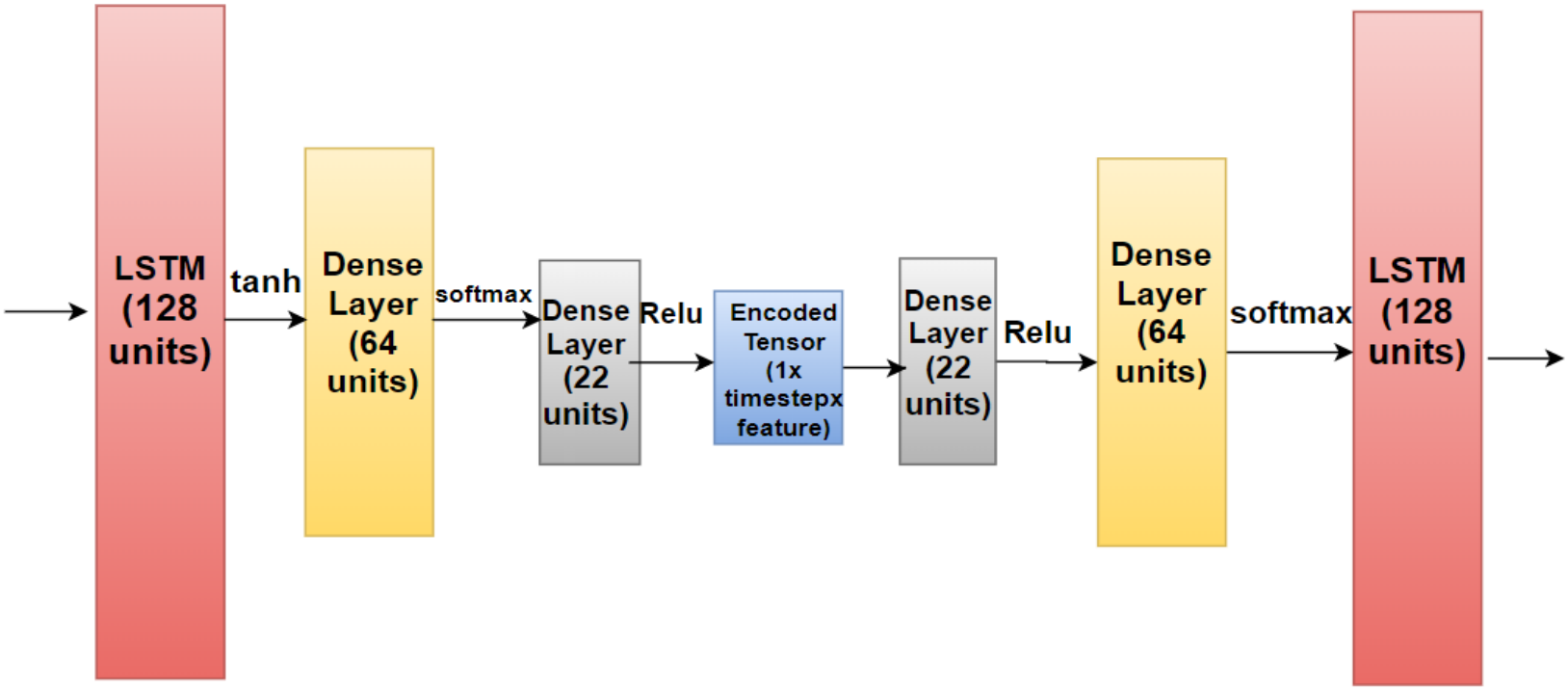
LSTM



- The full form is: Long short-term memory (LSTM)[10].
- Here the hidden state is computed as a function of the input sequences and not on the last input alone.

[10] Sepp Hochreiter and Jürgen Schmidhuber. "Long short-term memory". In: *Neural computation* 9.8 (1997), pp. 1735–1780.

LSTM Autoencoder



- This is the figure representation of the LSTM Autoencoder that we used to build LAC. We are directly inspired from[11] and[12].

[11] Nitish Srivastava, Elman Mansimov, and Ruslan Salakhudinov. "Unsupervised learning of video representations using lstms". In: *International conference on machine learning*. 2015, pp. 843–852.

[12] Aaron Tuor et al. "Deep learning for unsupervised insider threat detection in structured cybersecurity data streams". In: *Workshops at the Thirty-First AAAI Conference on Artificial Intelligence*. 2017.

Community Detection I

- Social, technological and information systems can often be described in terms of complex networks that have a topology of interconnected nodes combining organizations and randomness.
- On the basis of this interconnection and modularity we can easily deduct different communities in a dataset (we used CERT V6.2[13] and the email transaction data here to detect the graph).
- **Louvain Algorithm**[14]: It is a greedy algorithm that returns communities faster and most of the time without overlapping. It works on "Modularity".

[13] Joshua Glasser and Brian Lindauer. "Bridging the gap: A pragmatic approach to generating insider threat data". In: *2013 IEEE Security and Privacy Workshops*. IEEE. 2013, pp. 98–104.

[14] Vincent D Blondel et al. "Fast unfolding of communities in large networks". In: *Journal of statistical mechanics: theory and experiment* 2008.10 (2008), P10008.

Community Detection II

- Modularity is defined as follows -

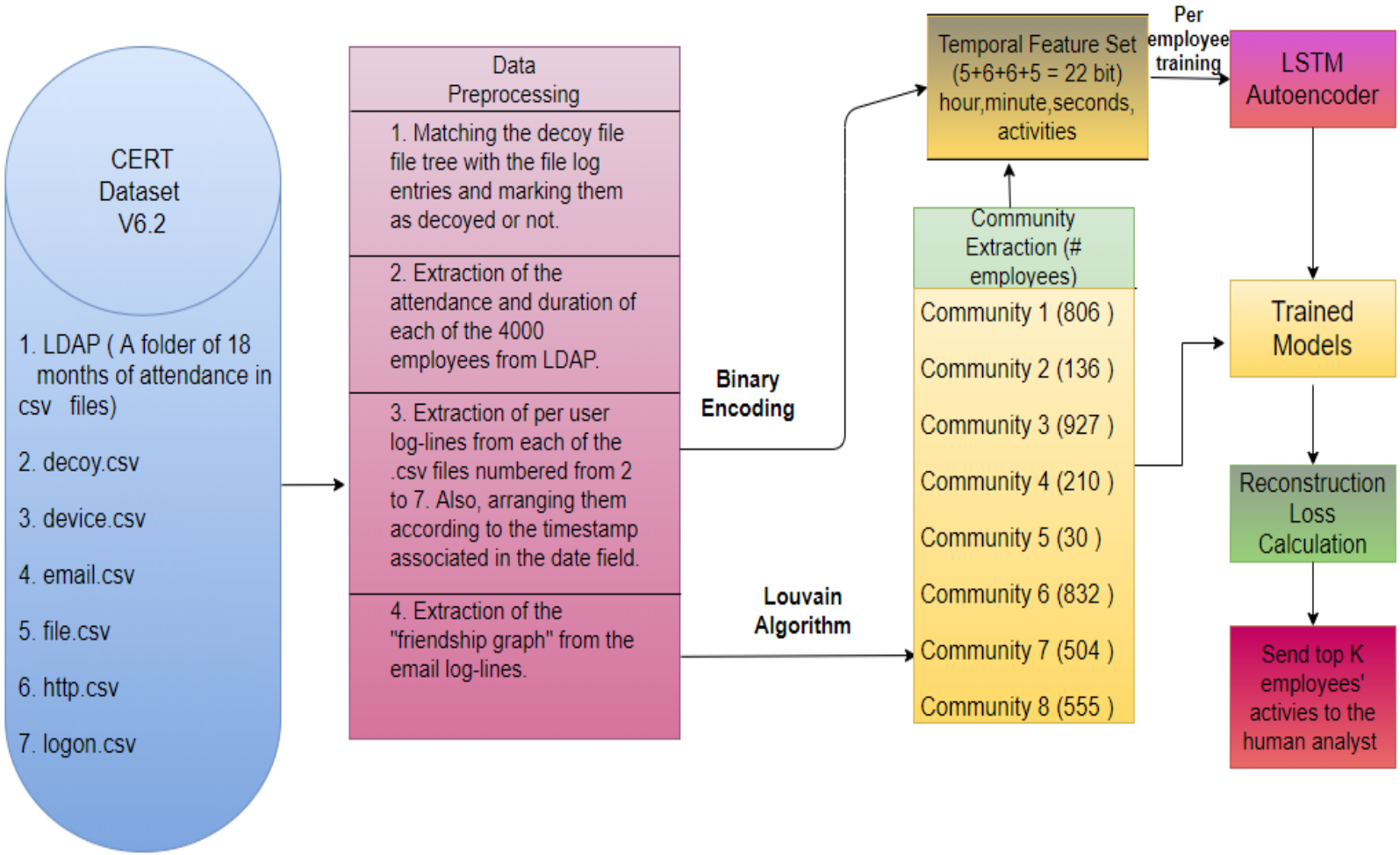
$$Q = \frac{1}{2m} \sum_{i,j} [A_{\mathrm{i,j}} - \frac{k_i k_j}{2m}] \delta(C_i, C_j)$$

  Here, $A_{\mathrm{i,j}}$ is the edge weight between nodes i and j; k_i and k_j are the sum of the weights of the edges attached to nodes i and j, respectively; m is the sum of all of the edge weights in the graph; c_i and c_j are the communities of the nodes; and δ is Kronecker delta function ($\delta_{\mathrm{x,y}} = 1$ if $x = y$, 0 otherwise).
- The algorithm will optimize[15] modularity and according to that modularity it will assign the nodes to their respective communities.

[15] Hao Lu, Mahantesh Halappanavar, and Ananth Kalyanaraman. "Parallel heuristics for scalable community detection". In: *Parallel Computing* 47 (2015), pp. 19–37.

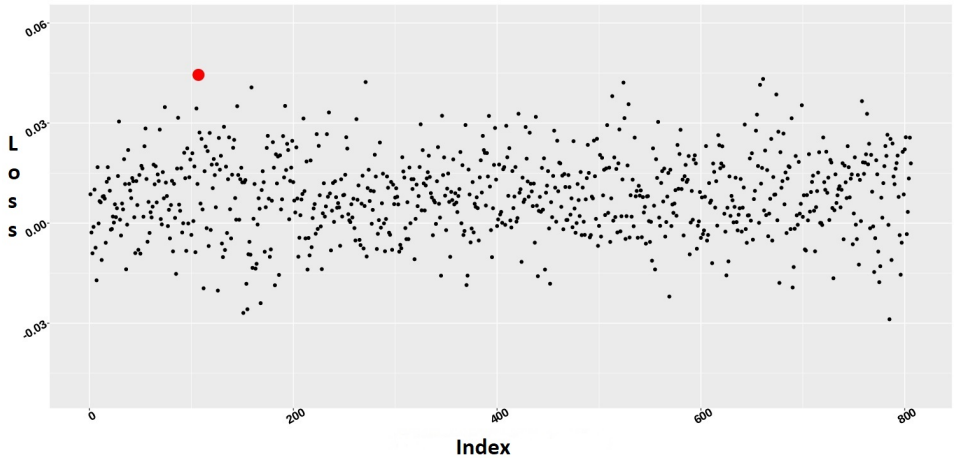
LAC: LSTM AUTOENCODER with Community for Insider Threat Detection (1)

- Flow- chart of LAC:

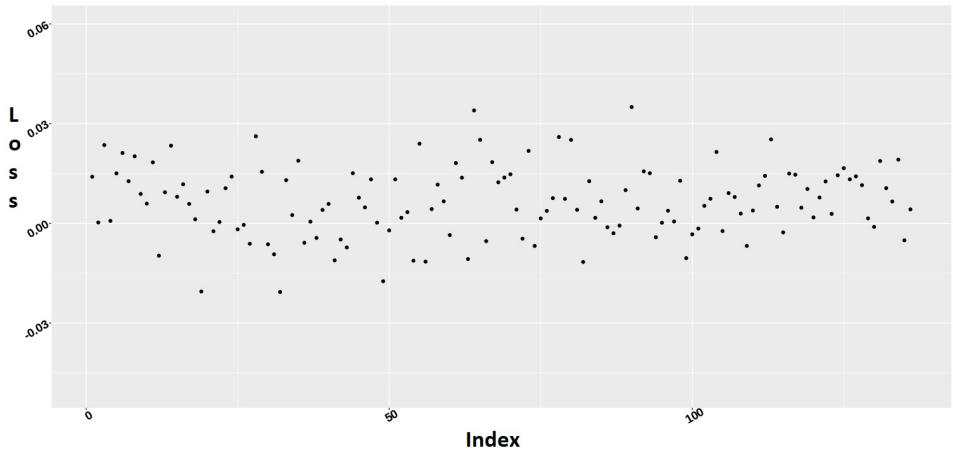


LAC: LSTM AUTOENCODER with Community for Insider Threat Detection (2)

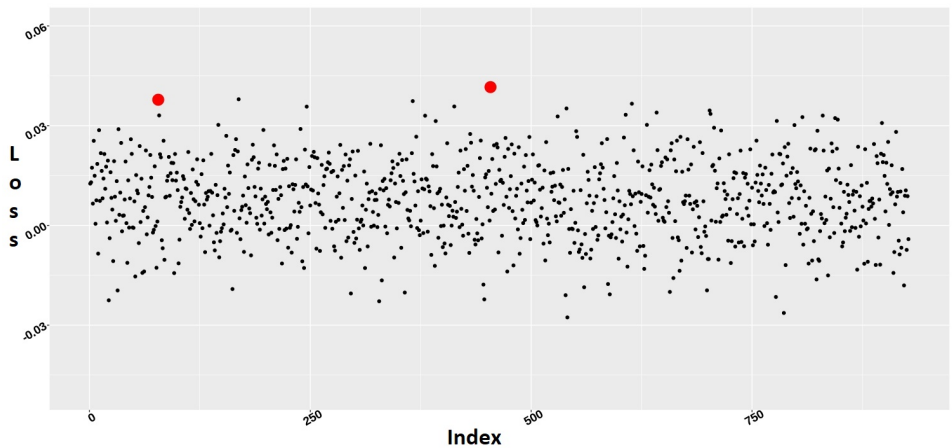
- Result part 1:



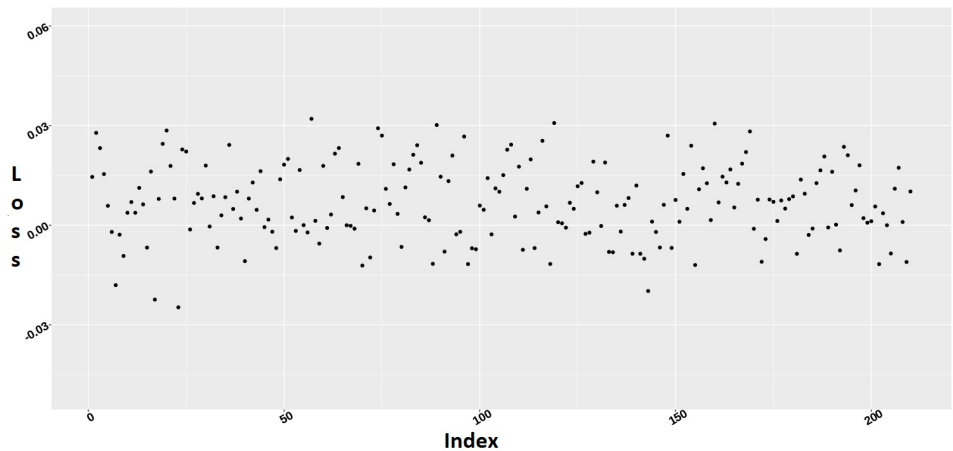
Community 1 Result



Community 2 results



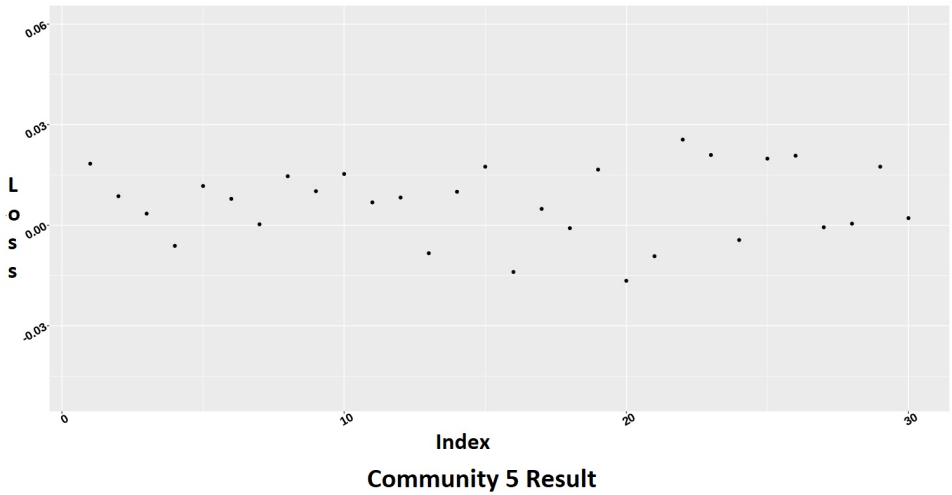
Community 3 Result



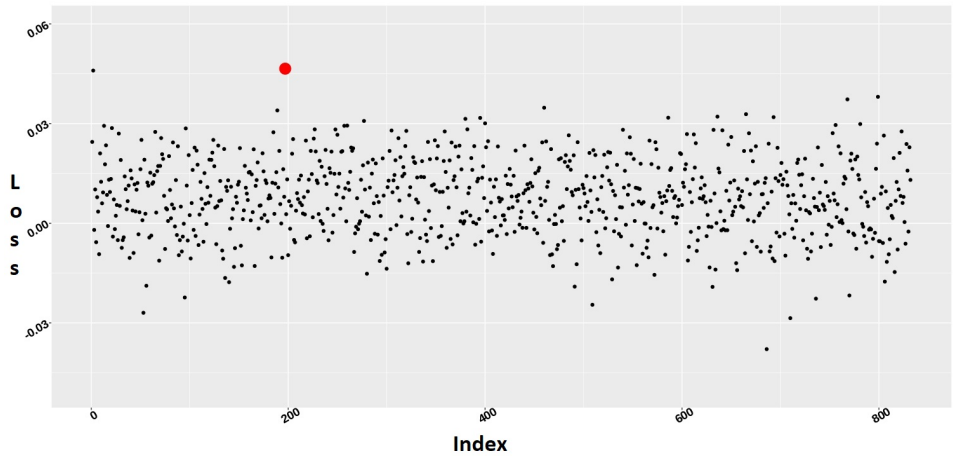
Community 4 Result

LAC: LSTM AUTOENCODER with Community for Insider Threat Detection (3)

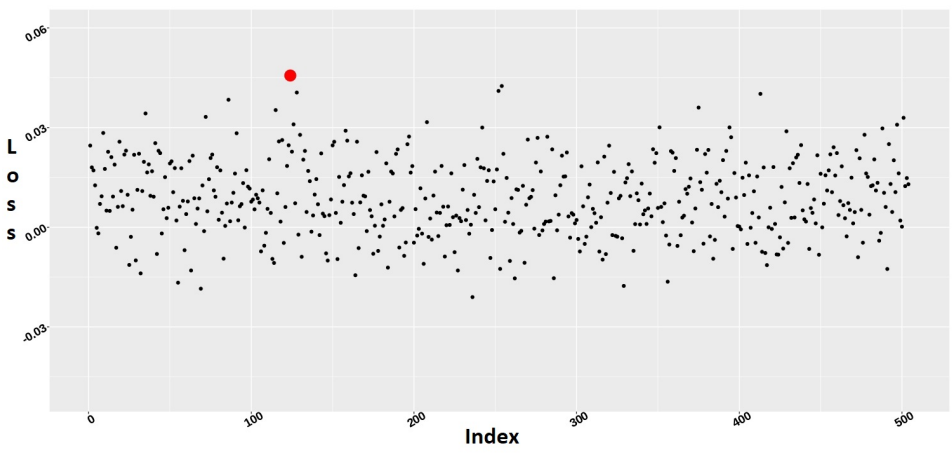
- Result part 2:



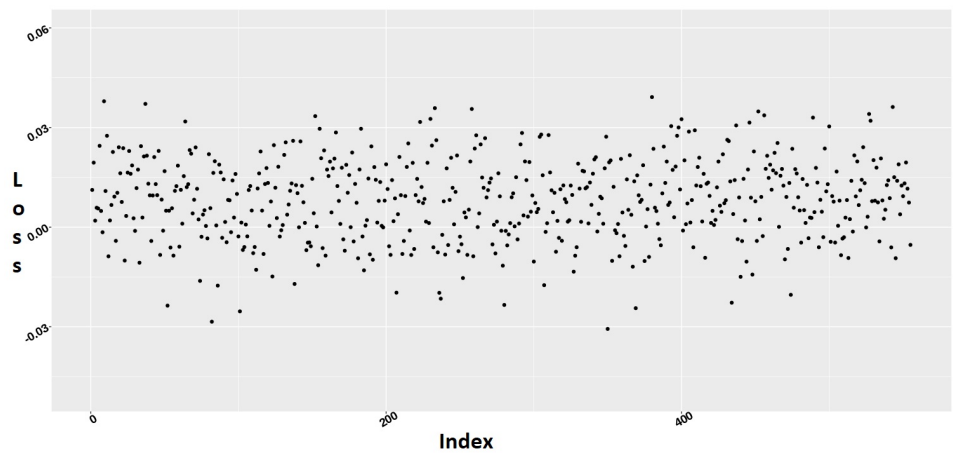
Community 5 Result



Community 6 Result



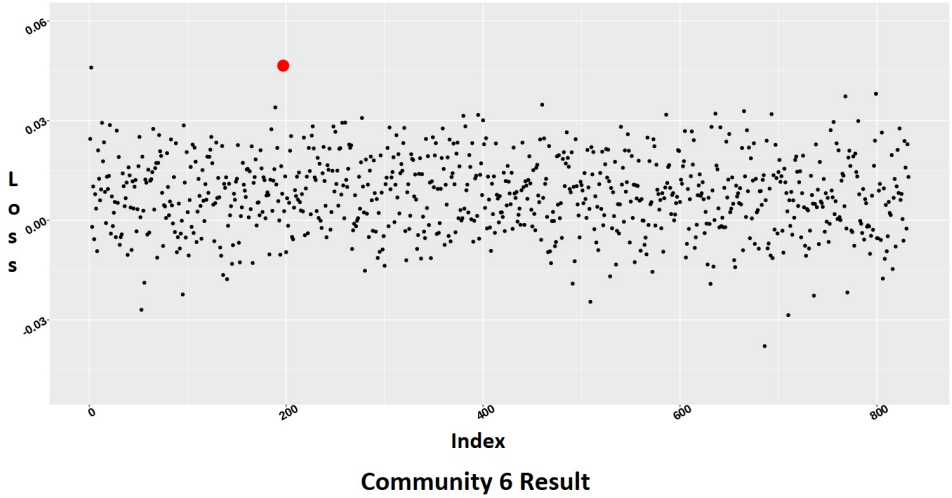
Community 7 Result



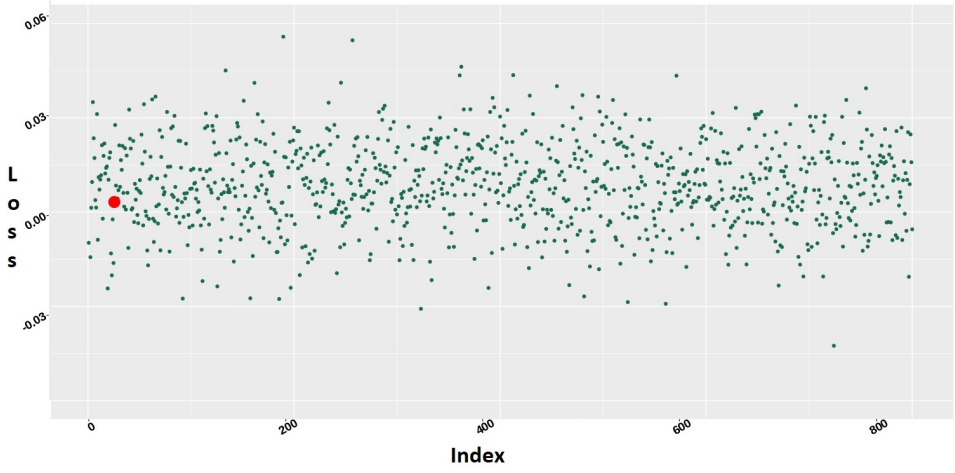
Community 8 result

LAC: LSTM AUTOENCODER with Community for Insider Threat Detection (4)

- Cross checking LAC over arbitrary 1000 users:



Community 6 Result



Randomly picked 1000 Employees

Future Direction

- Instead of using only one feature to detect the *Friendship Graph*, we will use other features too (e.g.. email content, web visit activities, file tree hierarchy etc.).
- We will try different community detection and clustering algorithm to find communities from different direction.
- We want to build an automated, differentially private and algorithmically fair community recommendation system on top of our approach.
- Instead of LSTM we want to try different networks to build the autoencoder.

Conclusion

- We propose LAC, a deep learning model using LSTM AUTOENCODER that is capable of reproducing the action sequences again with less reconstruction loss for the normal employees and greater reconstruction loss for the anomalous ones, with the help of its inherent capability to store temporal behavior in LSTM cell.
- Our novel approaches here are:
  - Usage of community of employees instead of analysis on a whole set.
  - Usage of LSTM AUTOENCODER to model the deep learning approach
  - Building feature set in the granularity of event occurrence with respect to activities

Thank You!!