Detecting Network Intrusion through Anomalous Packet Identification

Tanjim Munir Dipon

Md. Shohrab Hossain

Husnu S Narman

Outlines

- Motivation
- Problem Definition
- Methodology
- Implementation
- Result
- Future Works

Motivation

- Increasing communication through Internet, so increased risks of network attacks.
- Using packet capture files to extract information about different network sessions.
- Detecting anomalous sessions with no prior knowledge about their behaviour.
- Mitigating the risks of network attacks.

Problem Definition

What is Network Intrusion Detection?

- Procedure of detecting malicious traffic on the network on the basis of given rules or statistics.

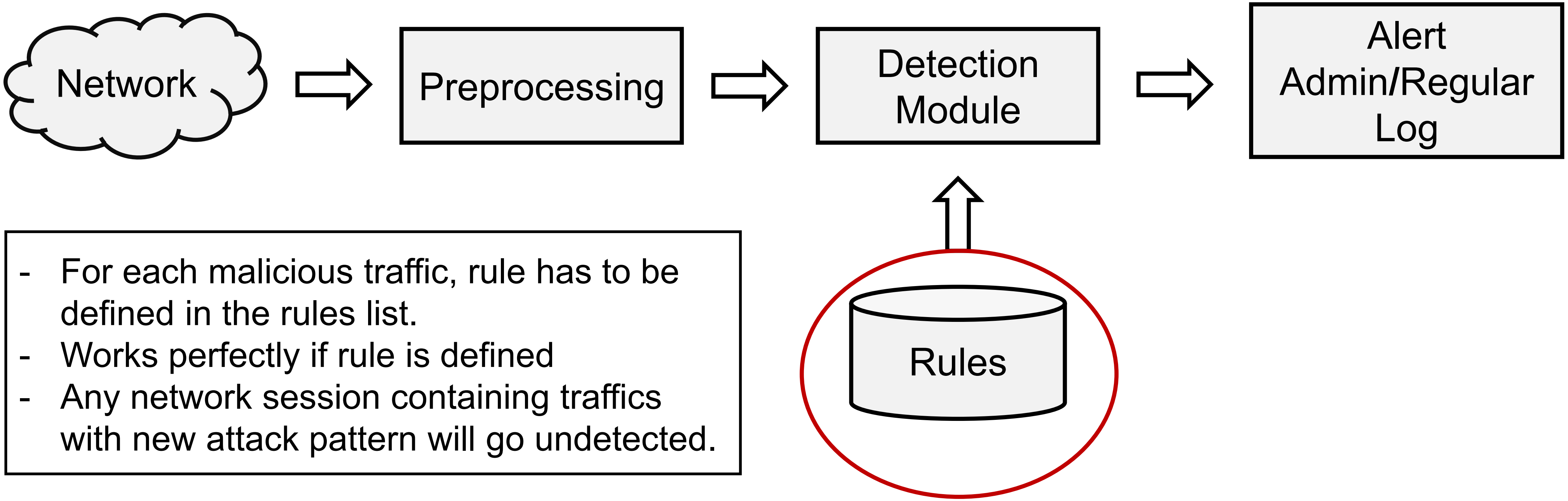
- Two types of detection scheme are possible;

Network Intrusion Detection → Signature/Rule Based

Network Intrusion Detection → Anomaly Based

Problem Definition

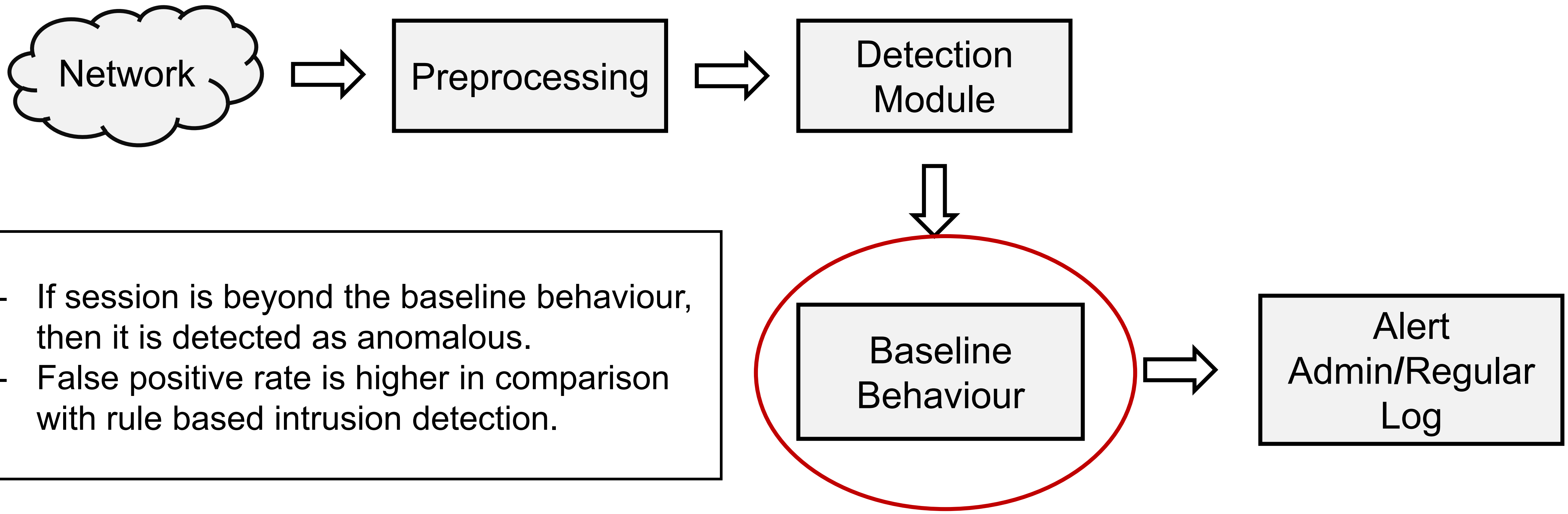
Signature based Intrusion Detection



- For each malicious traffic, rule has to be defined in the rules list.
- Works perfectly if rule is defined
- Any network session containing traffics with new attack pattern will go undetected.

Problem Definition

Anomaly based Intrusion Detection



- If session is beyond the baseline behaviour, then it is detected as anomalous.
- False positive rate is higher in comparison with rule based intrusion detection.

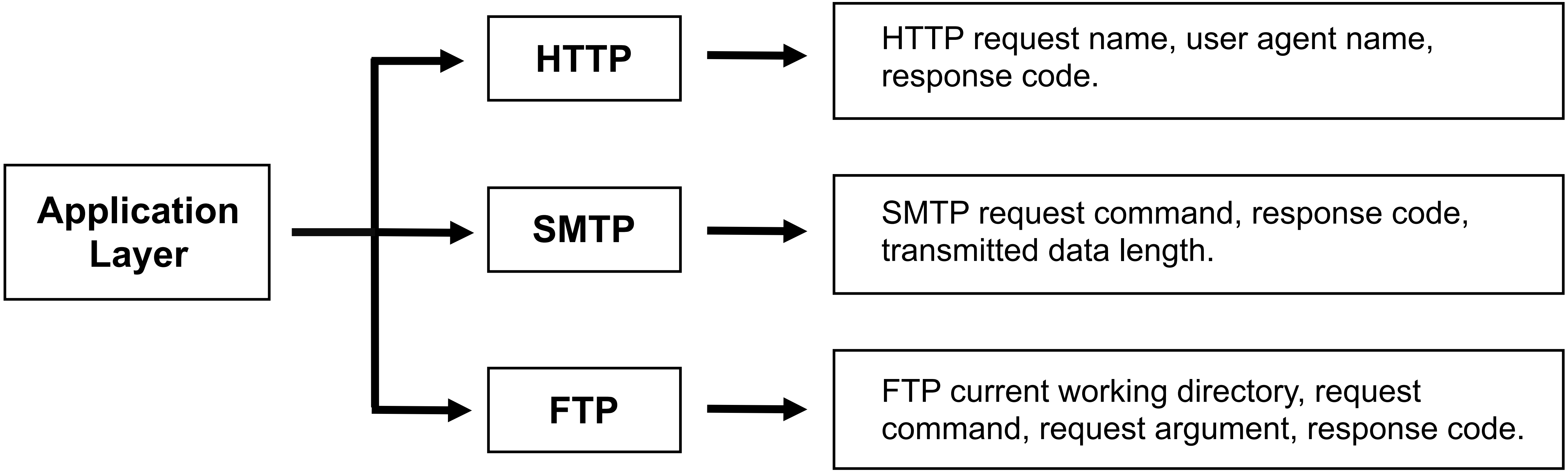
Methodology

- Data extraction from different services of network traffics.
- Reducing the dimensionality of the extracted data from network sessions.
- Clustering the sessions in all possible **3-**dimensions.
- Identifying the anomalous sessions on the basis of their outlier count in all possible combinations.

Implementation

Data Extraction from Network Traffic

- In this module, data is extracted from different protocols of network packets and then recorded as statistics inside corresponding sessions.



Implementation

Data Extraction from Network Traffic

Transport Layer (TCP) →

- Source and destination port numbers
- Average TCP segment length from client to server
- Average TTL value of SYN flagged packets
- SYN, SYN-ACK, PUSH, URG, RST and FIN flag percentage
- RST and FIN flag count from client to server and server to client.

Network Layer →

- Source and destination IP addresses
- Don’t and More Fragment rate
- ICMP packet type
- ICMP checksum status
- Avg. data length of ICMP packets

Implementation

Dimensionality Reduction

- Dimensionality reduction is applied to consider only the essential features in detecting anomalous sessions. Also any dependency in between the attributes is omitted.

Dimensionality Reduction → **Principal Component Analysis** → **Includes**

- Standardize the attributes to avoid any biasing.
- Calculate the co-variance matrix from the standardized data.
- Determine the eigenvalues and eigenvectors and take the eigenvectors with maximum variance.
- Project the sessions into the eigenvectors.

Implementation

Clustering and Outlier Marking

- Clustering is applied to all of the 3 combinations of the principal components and finally sessions having the most outlier count are recorded as anomalous.

Clustering and Outlier Detection

Includes

Create object with all possible 3 principal components

Apply Density based clustering to each object

Create Outlier count for each Session

Includes

- Cluster creation on the basis of core and border point determination.
- Label unreachable points as outliers

Results

- DARPA 1999 dataset is used to evaluate the proposed model. Anomalies detected in the dataset are given according to their respective protocols.

Network Layer

- Identical source and destination **IP** address.
- High amount of data transmitted through ICMP packets to the server.
- High amount of checksum errors.
- Request with no responses from the server.
- High amount of **TTL** values.

Attacks included
➢ Ping of Death ➢ Land

Results

Transport Layer

- High amount of data transmission through **TCP** bookkeeping packets.
- High amount of **RST** and **FIN** flag rate per session from server to client and client to server.
- High difference between **SYN** and **SYN-ACK** flag rate per session.
- **RST** and **FIN** flags with no **SYN** and **SYN-ACK** flags in a session.

Attacks included

- Back
- SYN Flood
- Portsweep

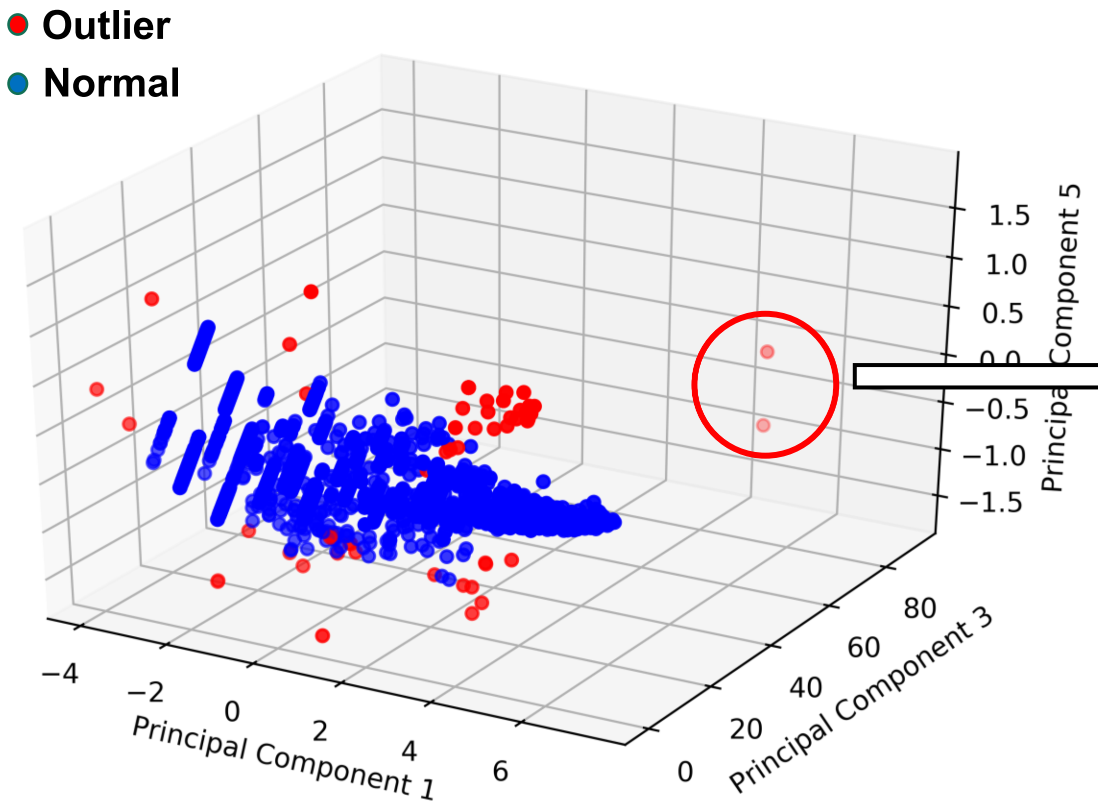
Results

Application Layer

- High amount of data transmitted as **HTTP** user agent through **TCP** bookkeeping packets.
- No **SMTP** session starting or closing command yet tried to transmit a lot of data.
- A lot amount of data transmitted in **SMTP** session with many packets full to **TCP** segment capacity.
- Trying to append a file to the **FTP** root directory with anonymous session.

Attacks included
➢ Apache2 ➢ Sendmail ➢ PP-Macro ➢ FTP-Write

Results



- All of the different clusters are shown with several bunch of blue points. These clusters show the normal **HTTP** sessions.

- Red points are recorded as outliers.
- Similar graph is achieved for all 3-combinations of principal components.
- Finally sessions those appear as outlier in most of these combinations are declared as anomalous.

HTTP Sessions as data points concerning principle components 1, 3 and 5

Future Works

- Process other services such as Telnet, UDP, SNMP, encrypted traffics for a wide range of detection.
- Use other datasets to evaluate the performance of the system in a more robust way.
- Automating the entire procedure through assigning the hyper parameter values automatically.

References

[1] M. A. Jonas, R. Islam, M. S. Hossain, H. S. Narman, and M. Atiquzzaman, “An intelligent system for preventing ssl stripping-based session hijacking attacks,” in *IEEE Military Communications (MILCOM)*. Norfolk, VA, USA: IEEE, 12-14 Nov., 2019.

[2] M. I. Ashiq, P. Bhowmick, M. S. Hossain, and H. S. Narman, “Domain flux based dga botnet detection using feedforward neural network,” in *IEEE Military Communications (MILCOM)*. Norfolk, VA, USA: IEEE, 12-14 Nov., 2019.

[3] P. Casas, J. Mazel, and P. Owezarski, “Unada: Unsupervised network anomaly detection using sub-space outliers ranking,” in *International Conference on Research in Networking*. Berlin, Germany: Springer, May 9., 2011, pp. 40–51.

[4] J. Dromard, G. Roudiere, and P. Owezarski, “Online and scalable unsupervised network anomaly detection method,” *IEEE Transactions on Network and Service Management*, vol. 14, no. 1, pp. 34–47, 09 November., 2016.

[5] I. Savvas, A. Chernov, M. Butakova, and C. Chaikalis, “Increasing the quality and performance of n-dimensional point anomaly detection in traffic using pca and dbscan,” in *26th Telecommunications Forum (TELFOR)*. Belgrade, Serbia: IEEE, 20-21 Nov., 2018, pp. 1–4.

[6] X. Zhao, G. Wang, and Z. Li, “Unsupervised network anomaly detection based on abnormality weights and subspace clustering,” in *Sixth International Conference on Information Science and Technology (ICIST)*. Dalian, China: IEEE, 6-8 May., 2016, pp. 482–486.

[7] M. Z. Alom and T. M. Taha, “Network intrusion detection for cyber security using unsupervised deep learning approaches,” in *National Aerospace and Electronics Conference (NAECON)*. Dayton, OH, USA: IEEE, 27-30 June., 2017, pp. 63–69.

[8] D. S. Terzi, R. Terzi, and S. Sagiroglu, “Big data analytics for network anomaly detection from netflow data,” in *International Conference on Computer Science and Engineering (UBMK)*. Antalya, Turkey: IEEE, 5-8 Oct., 2017, pp. 592–597.

[9] Z. Chen and Y. F. Li, “Anomaly detection based on enhanced dbscan algorithm,” *Procedia Engineering*, vol. 15, pp. 178–182, 1 Jan., 2011.

[10] Z. Chen, C. K. Yeo, B. S. L. Francis, and C. T. Lau, “Combining mic feature selection and feature-based mspca for network traffic anomaly detection,” in *Third International Conference on Digital Information Processing, Data Mining, and Wireless Communications (DIPDMWC)*. Moscow, Russia: IEEE, 6-8 July., 2016, pp. 176–181.

[11] W. Chen, F. Kong, F. Mei, G. Yuan, and B. Li, “A novel unsupervised anomaly detection approach for intrusion detection system,” in *IEEE 3rd international conference on big data security on cloud (BigDataSecurity)*. Beijing, China: IEEE, 26-28 May., 2017, pp. 69–73.

[12] M. Odiathevar, W. K. Seah, and M. Frean, “A hybrid online offline system for network anomaly detection,” in *28th International Conference on Computer Communication and Networks (ICCCN)*. Valencia, Spain: IEEE, 29 July-1 Aug., 2019, pp. 1–9.

[13] M. T. Hossain, M. S. Hossain, and H. S. Narman, “Detection of undesired events on real-world scada power system through process monitoring,” in *11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*. New York, NY, USA: IEEE, 28-31 Oct., 2020.

[14] “DARPA intrusion detection evaluation dataset,” 1999, https://archive.ll.mit.edu/ideval/data/1999data.html.


Thank You!