False Data Injection Attack Dataset for Industrial Internet of Things

This dataset contains one .csv file. The dataset has 26 features that are “http_response_body_len”, “dst_port”, “dns_rcode”, “dns_qclass”, ” dns_qtype”, ” src_port”, “ http_resp_mime_types”, ”http_request_body_len”, “conn_state”, “http_user_agent”, ” ssl_issuer”, ” ssl_subject”, ” http_orig_mime_types”, ” http_trans_depth”, “http_method”, “http_status_code”, ” http_version”, ” http_uri”, ” ssl_cipher”, ” ssl_version”, “ssl_resumed”, “ssl_established”, ” proto”, ” dns_rejected”, ” dns_RA”, ” dns_RD”, “dns_AA”, “service”, ” dns_query”, ” dst_ip_bytes”.

During the training process dataset head is present like Fig.1.

```
df.head()
```

Out[3]:

	http_response_body_len	dst_port	dns_rcode	dns_qclass	dns_qtype	src_port	http_resp_mime_types	http_request_body_len	conn_state	http_user_agent
0	0.019536	0.086357	0.495797	0.041017	0.194625	0.183797	0.7	0.880951	0.217391	0.972222
1	0.019536	0.188415	0.484033	0.047996	0.212062	0.394561	0.7	0.880955	0.217391	0.972222
2	0.019536	0.086357	0.495797	0.041017	0.194625	0.183797	0.7	0.880951	0.217391	0.972222
3	0.019536	0.188415	0.484033	0.047996	0.212062	0.394561	0.7	0.880955	0.217391	0.972222
4	0.019535	0.004710	0.505208	0.035434	0.180676	0.015186	0.7	0.880948	0.217391	0.972222

5 rows × 31 columns

The total number of data scenarios is presented in Fig. 2.

```
In [6]: df['marker'].value_counts()

Out[6]: Natural    8688
        Attack     6737
        Name: marker, dtype: int64
```

To validate cybersecurity applications especially false data injection (FDI) attack, this study introduces IIoT datasets and their analysis.