Is Encrypted Client Hello (ECH) a Challenge for Traffic Classification?

Presented by - Devendra Pratap Singh

2101AI13

TLS Handshake Phases

- **Key Exchange**
    - Client sends ClientHello (CH) with TLS parameters.
    - Server responds with ServerHello (SH) to compute shared encryption secrets.
- **Server Parameters**
    - Server sends remaining parameters in an EncryptedExtensions (EE) message.
- **Authentication**
    - Parties authenticate via Certificate exchange and complete the handshake.

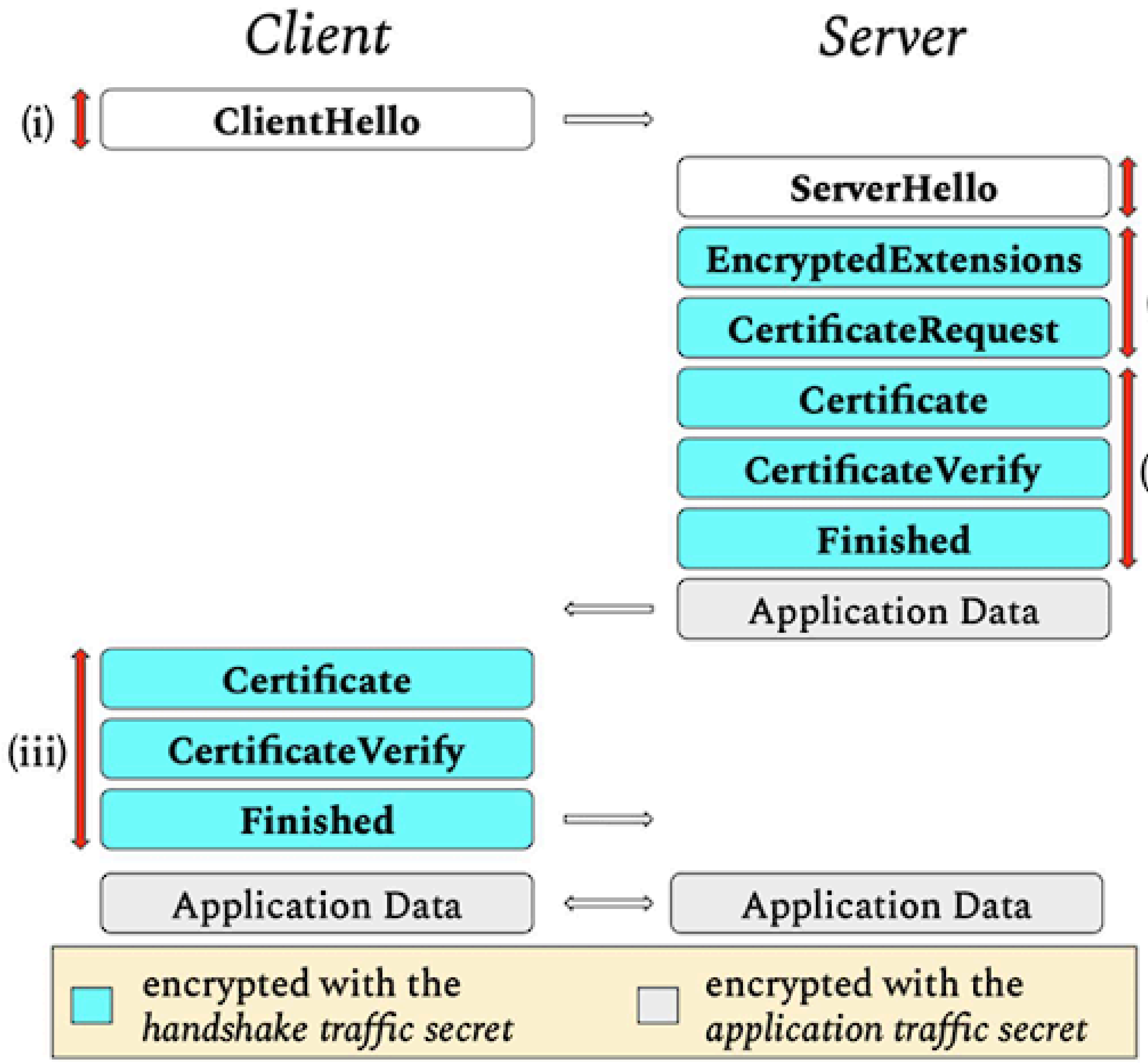
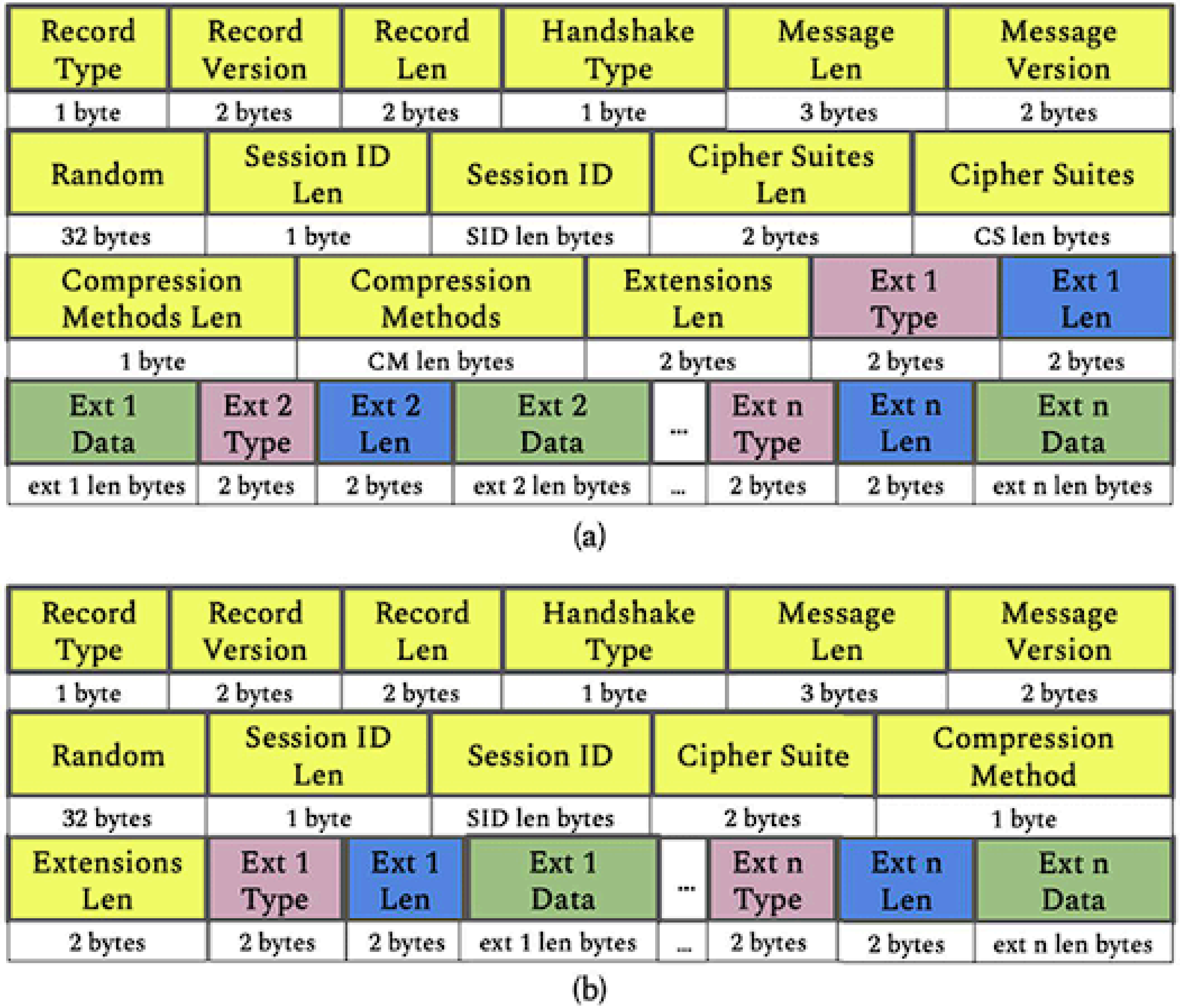


FIGURE 1. Three phases of the TLS 1.3 handshake protocol: (i) Key exchange, (ii) Server parameters and (iii) Authentication.



Record Type	Record Version	Record Len	Handshake Type	Message Len	Message Version
1 byte	2 bytes	2 bytes	1 byte	3 bytes	2 bytes

Random	Session ID Len	Session ID	Cipher Suites Len	Cipher Suites
32 bytes	1 byte	SID len bytes	2 bytes	CS len bytes

Compression Methods Len	Compression Methods	Extensions Len	Ext 1 Type	Ext 1 Len
1 byte	CM len bytes	2 bytes	2 bytes	2 bytes

Ext 1 Data	Ext 2 Type	Ext 2 Len	Ext 2 Data	...	Ext n Type	Ext n Len	Ext n Data
ext 1 len bytes	2 bytes	2 bytes	ext 2 len bytes	...	2 bytes	2 bytes	ext n len bytes

(a)

Record Type	Record Version	Record Len	Handshake Type	Message Len	Message Version
1 byte	2 bytes	2 bytes	1 byte	3 bytes	2 bytes

Random	Session ID Len	Session ID	Cipher Suite	Compression Method
32 bytes	1 byte	SID len bytes	2 bytes	1 byte

Extensions Len	Ext 1 Type	Ext 1 Len	Ext 1 Data	...	Ext n Type	Ext n Len	Ext n Data
2 bytes	2 bytes	2 bytes	ext 1 len bytes	...	2 bytes	2 bytes	ext n len bytes

(b)

FIGURE 2. **(a) ClientHello and (b) ServerHello message structure.**

Evolution of TLS

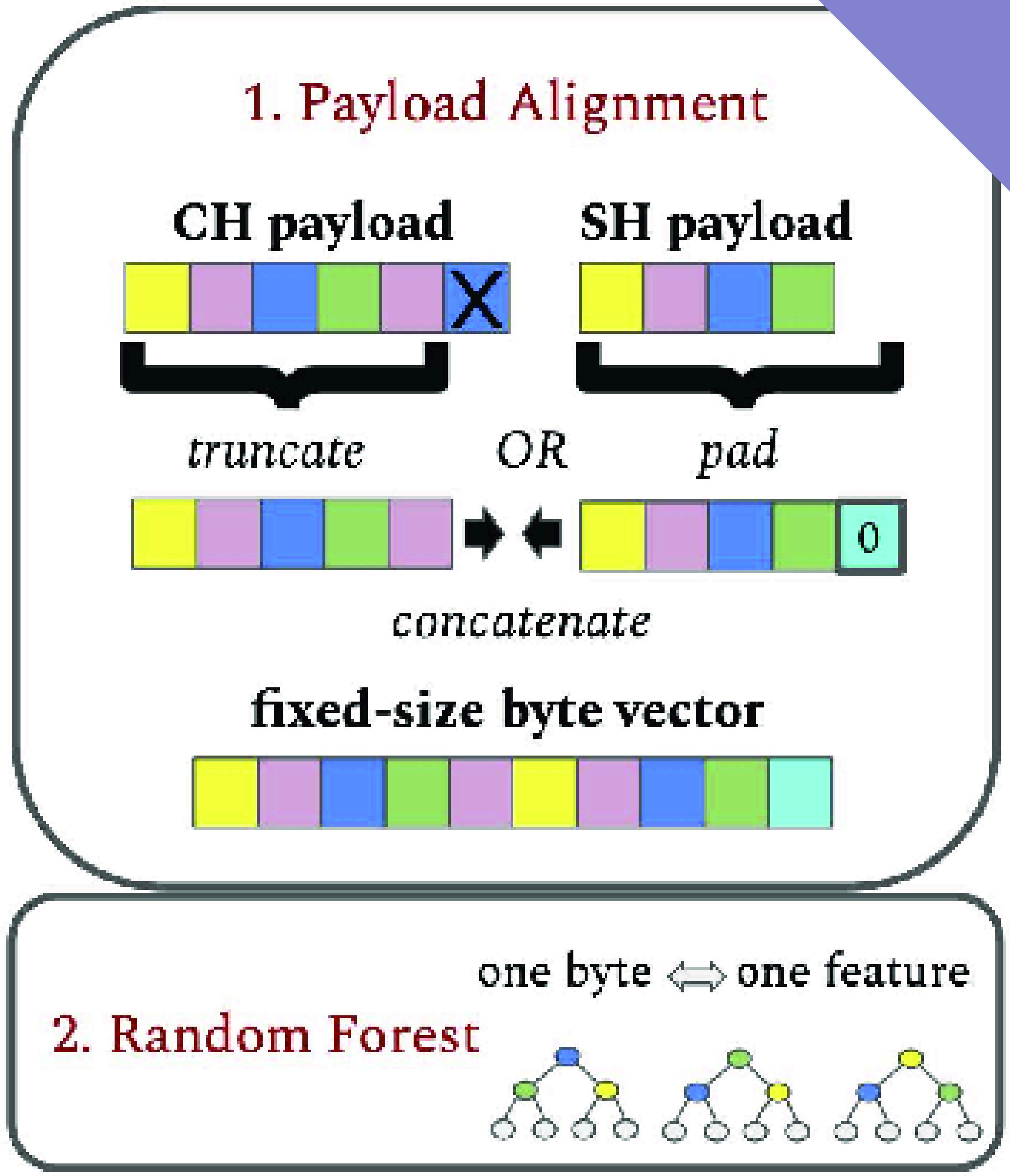
Feature	TLS 1.3 (ESNI)	ECH (Encrypted ClientHello)
Handshake Encryption	Partially encrypted (CH, SH unencrypted)	CHI encrypted (sensitive data hidden) **Unencrypted Fields**: Key share, pre-shared key, supported versions.
ClientHello (CH)	Unencrypted	Split into ClientHelloOuter (CHO) and ClientHelloInner (CHI)
ServerHello (SH)	Unencrypted	Same as TLS 1.3
Sensitive Extensions	Encrypted (Only the **SNI**)	SNI and ALPN encrypted in CHI

Aligned Bytes Random Forest (AB-RF)

Payload Alignment: Extracts exactly B bytes from the payload of each message (CH and SH), truncating or padding with zeros, and concatenates them into a single vector.

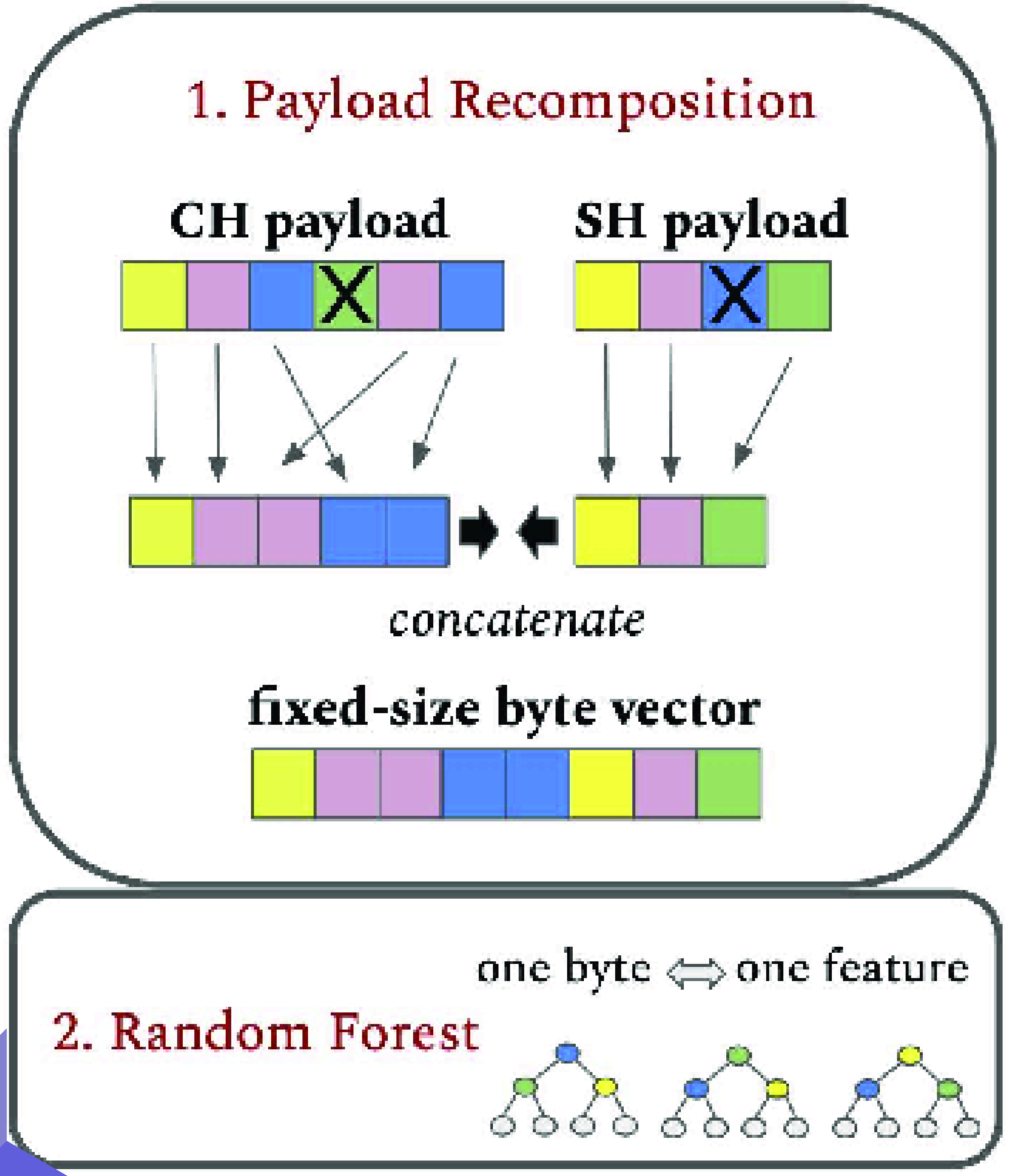
Random Forest: Uses the aligned bytes as a feature vector, builds D decision trees during training, and predicts traffic class based on decisions across all trees.

- Number of decision trees is varied.
- Number of features is set to 35.
- Evaluated with an aligned payload length of 185 bytes, which offers the lowest error rate.



a) AB-RF

Recomposed-Bytes Random Forest (RB-RF)



b) RB-RF

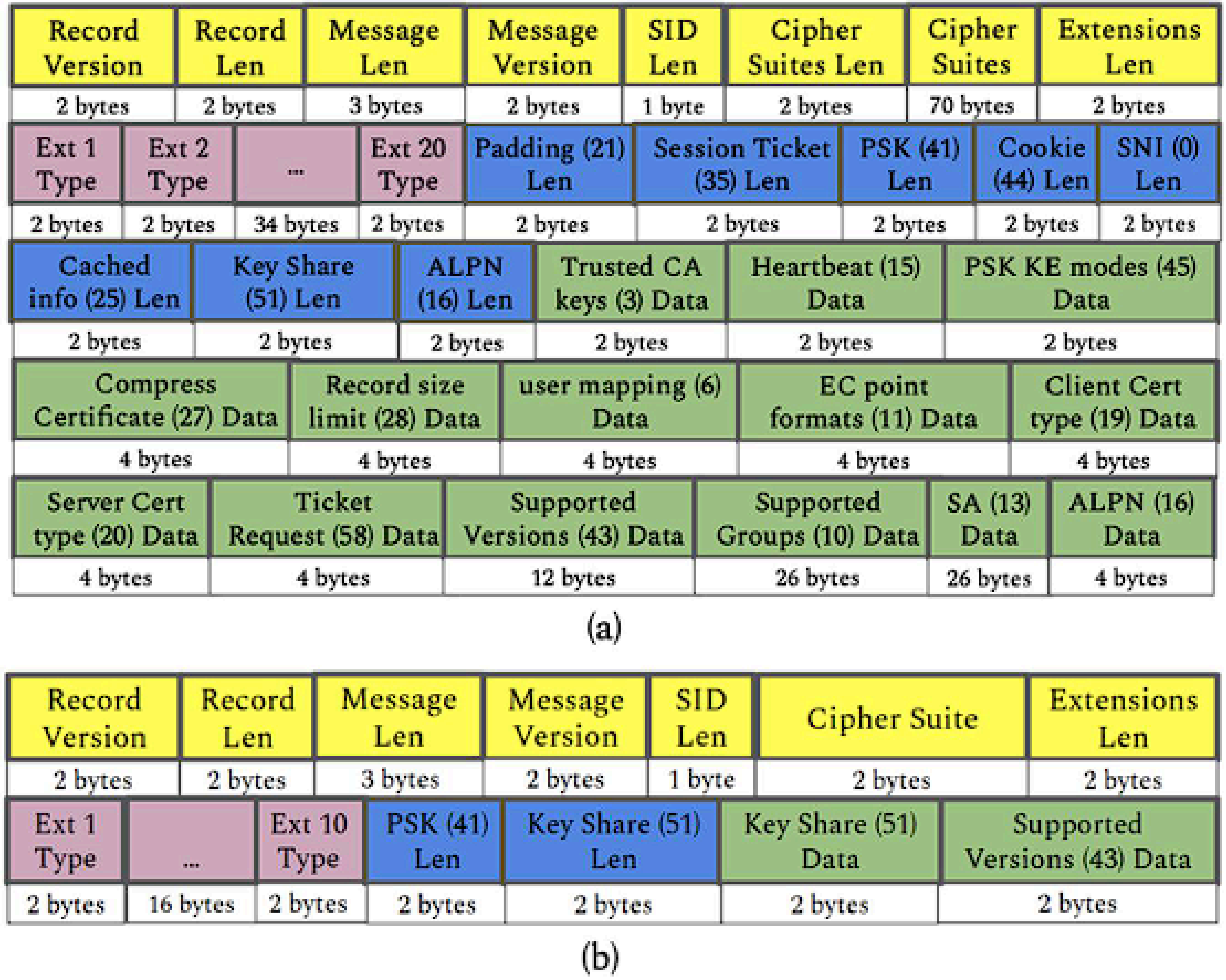
It improves classification by rearranging payload parameters, assigning fixed positions and lengths to them.

Decomposition:

Breaks down CH and SH messages into fields, extension types, lengths, and data.

New Composition

Parameters are selected and assigned fixed-length representations in a specific order.The recomposed payload contains four blocks: **field values, extension types, extension lengths, and selected extension contents.**



Record Version	Record Len	Message Len	Message Version	SID Len	Cipher Suites Len	Cipher Suites	Extensions Len
2 bytes	2 bytes	3 bytes	2 bytes	1 byte	2 bytes	70 bytes	2 bytes

Ext 1 Type	Ext 2 Type	...	Ext 20 Type	Padding (21) Len	Session Ticket (35) Len	PSK (41) Len	Cookie (44) Len	SNI (0) Len
2 bytes	2 bytes	34 bytes	2 bytes	2 bytes	2 bytes	2 bytes	2 bytes	2 bytes

Cached info (25) Len	Key Share (51) Len	ALPN (16) Len	Trusted CA keys (3) Data	Heartbeat (15) Data	PSK KE modes (45) Data
2 bytes	2 bytes	2 bytes	2 bytes	2 bytes	2 bytes

Compress Certificate (27) Data	Record size limit (28) Data	user mapping (6) Data	EC point formats (11) Data	Client Cert type (19) Data
4 bytes	4 bytes	4 bytes	4 bytes	4 bytes

Server Cert type (20) Data	Ticket Request (58) Data	Supported Versions (43) Data	Supported Groups (10) Data	SA (13) Data	ALPN (16) Data
4 bytes	4 bytes	12 bytes	26 bytes	26 bytes	4 bytes

(a)

Record Version	Record Len	Message Len	Message Version	SID Len	Cipher Suite	Extensions Len
2 bytes	2 bytes	3 bytes	2 bytes	1 byte	2 bytes	2 bytes

Ext 1 Type	...	Ext 10 Type	PSK (41) Len	Key Share (51) Len	Key Share (51) Data	Supported Versions (43) Data
2 bytes	16 bytes	2 bytes	2 bytes	2 bytes	2 bytes	2 bytes

(b)

FIGURE 7. (a) ClientHello and (b) ServerHello recomposed payload structure.

Data Preprocessing for TC Protocols

- **TLS Handshake Data Extraction**
  - Scapy is used to extract L4 (transport layer) payloads from packets carrying Client Hello (CH) and Server Hello (SH) messages.
  - Only CH and SH packets are considered, as packets beyond TLS 1.3 are encrypted and do not improve classification quality.
  - Server Certificate message (third packet) is used only for baseline classifier validation on Open HTTPS datasets.
  - QUIC flows and L3/lower-layer headers are excluded due to potential dataset biases.

- **Random Field Modification:**
  - The first 4 bytes of the random fields in CH and SH are replaced with zeros to avoid time/date biases in the dataset.

Models of Encryption Scenarios

- **ESNI (Encrypted SNI)**
  - Conceals only the SNI value, not its length.
  - CH payload is extracted from the first packet, and SNI is hidden by replacing it with zeros.
- **ECH (Encrypted ClientHello)**
  - Represents the strongest encryption where all CH extensions (except key share, pre-shared key, supported versions) are removed.
  - CH fields like Extensions Length, Record Length, and Message Length are updated based on removed extensions.
- **Common**
  - SH payload is extracted from the second packet.

WNL TLS Dataset

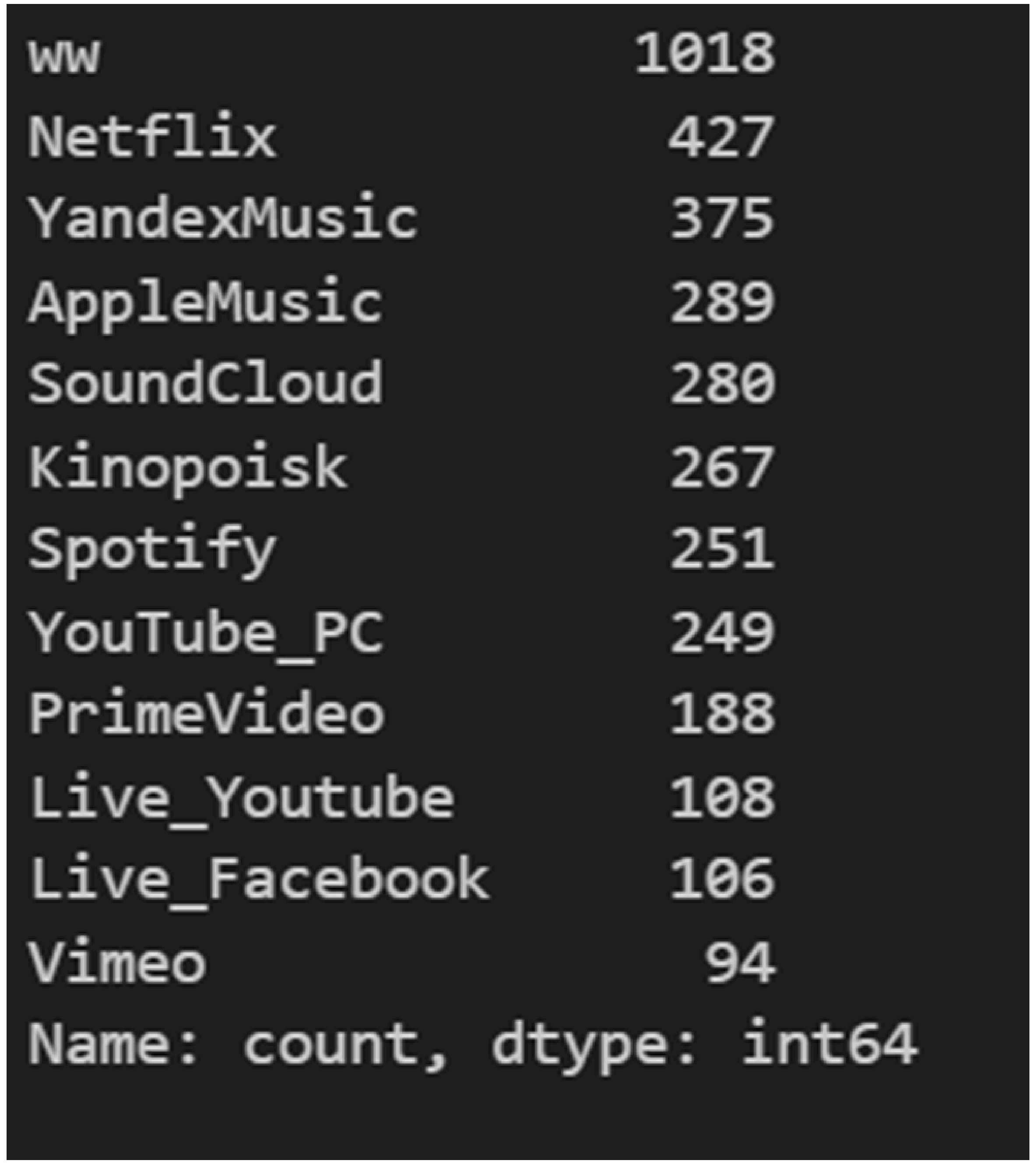
The dataset contains download traces of TLS-encrypted flows of four traffic types: buffered video, buffered audio, uplink live video streaming, and web.

ESNI

Extracted the payload from first packet of the flow and hide the SNI extension with zeroes

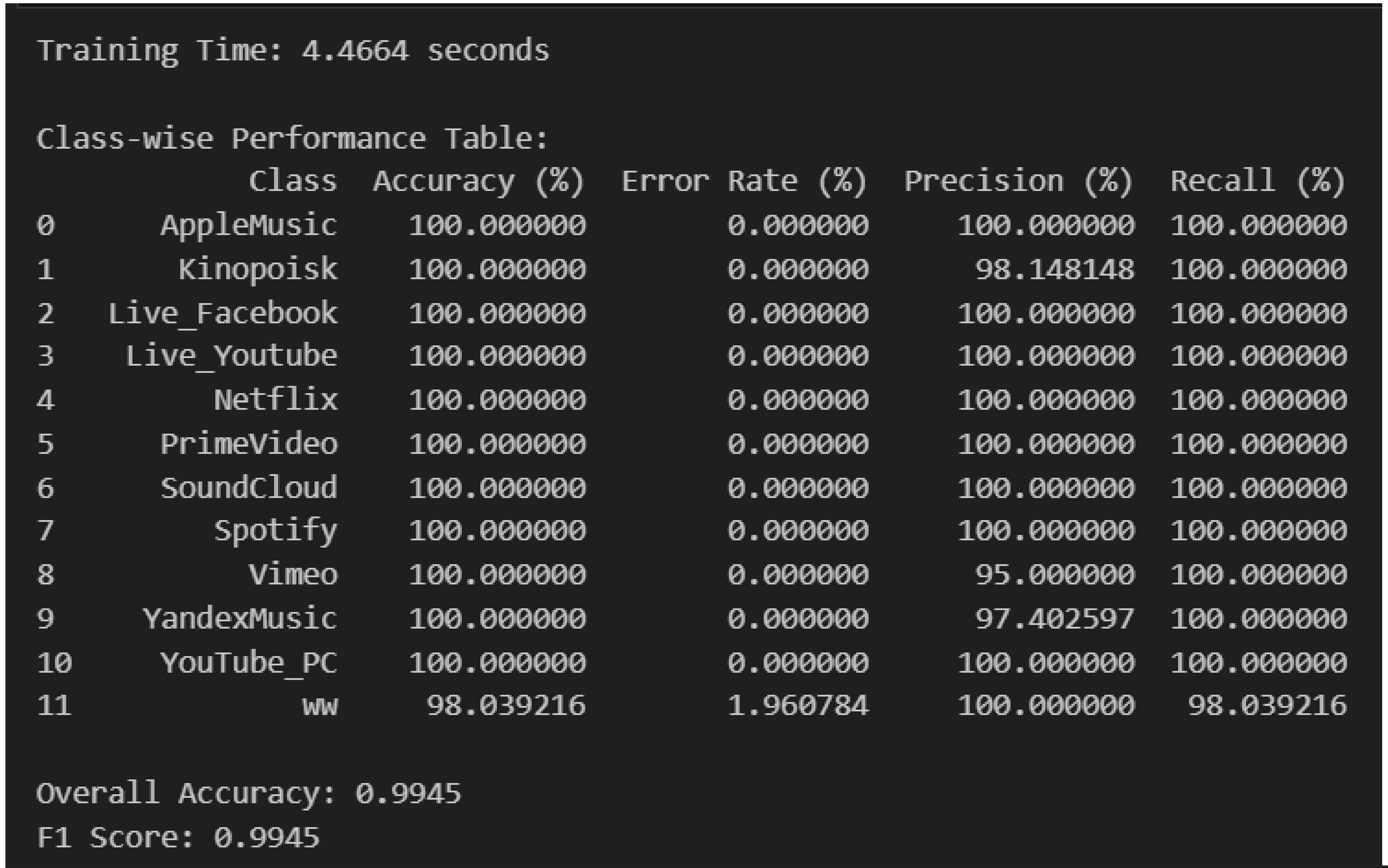
ECH

Extracted the CH payload and remove bytes corresponding to all CH extensions registered by IANA except for the ones that cannot be encrypted: key share, pre-shared key, and supported versions. Also, updated the Extensions Length, Record Lenght, Message Lenght fields of the CH

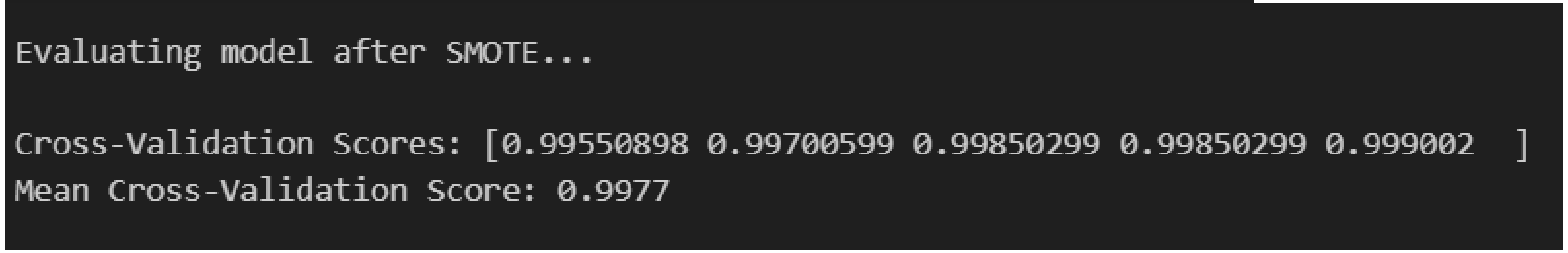


```
ww               1018
Netflix           427
YandexMusic       375
AppleMusic        289
SoundCloud        280
Kinopoisk         267
Spotify           251
YouTube_PC        249
PrimeVideo        188
Live_Youtube      108
Live_Facebook     106
Vimeo              94
Name: count, dtype: int64
```

Result of AB-RF on ESNI Dataset

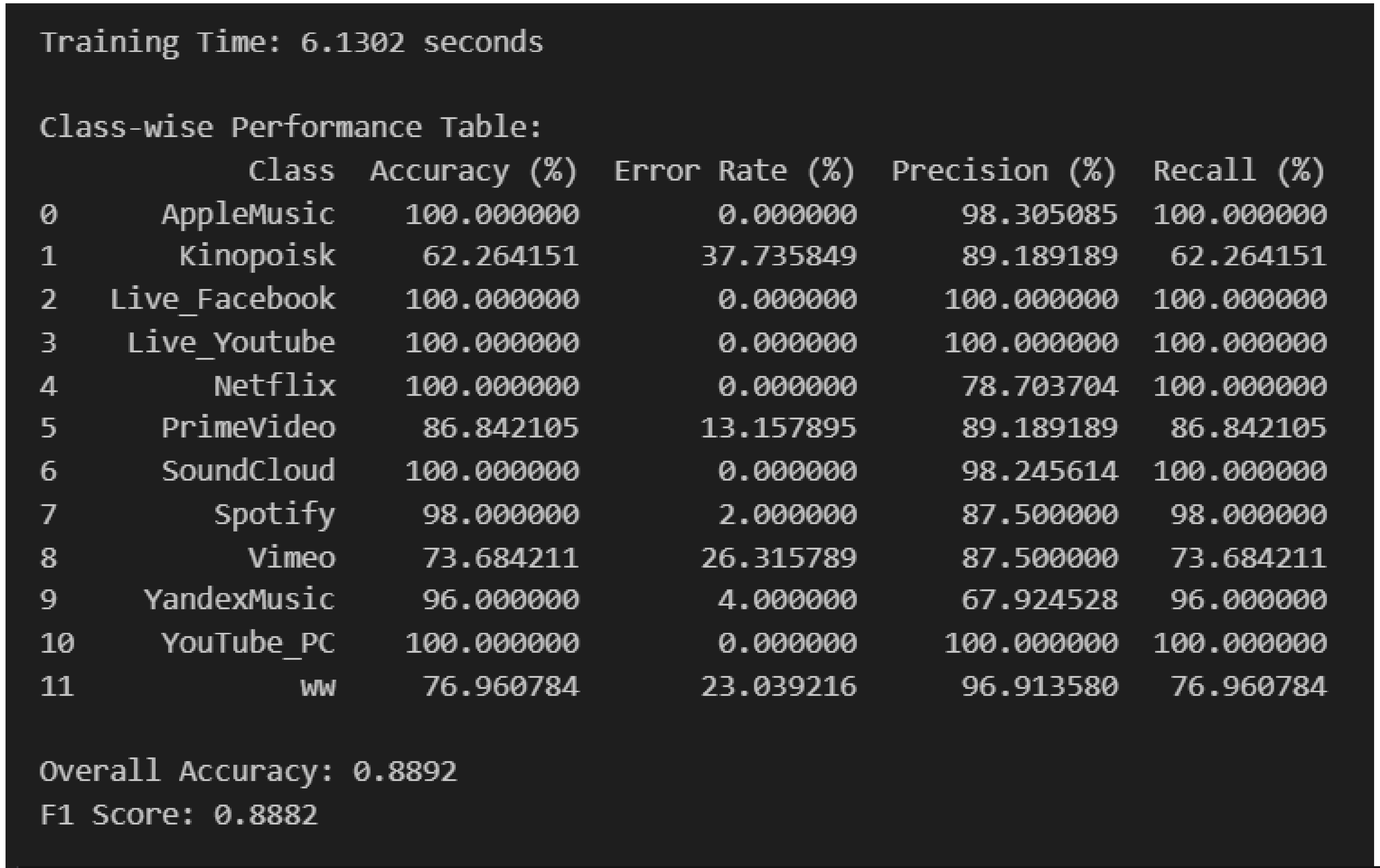


```
Training Time: 4.4664 seconds

Class-wise Performance Table:
           Class  Accuracy (%)  Error Rate (%)  Precision (%)  Recall (%)
0     AppleMusic    100.000000        0.000000     100.000000  100.000000
1      Kinopoisk    100.000000        0.000000      98.148148  100.000000
2  Live_Facebook    100.000000        0.000000     100.000000  100.000000
3   Live_Youtube    100.000000        0.000000     100.000000  100.000000
4        Netflix    100.000000        0.000000     100.000000  100.000000
5     PrimeVideo    100.000000        0.000000     100.000000  100.000000
6     SoundCloud    100.000000        0.000000     100.000000  100.000000
7        Spotify    100.000000        0.000000     100.000000  100.000000
8          Vimeo    100.000000        0.000000      95.000000  100.000000
9    YandexMusic    100.000000        0.000000      97.402597  100.000000
10    YouTube_PC    100.000000        0.000000     100.000000  100.000000
11            ww     98.039216        1.960784     100.000000   98.039216

Overall Accuracy: 0.9945
F1 Score: 0.9945
```

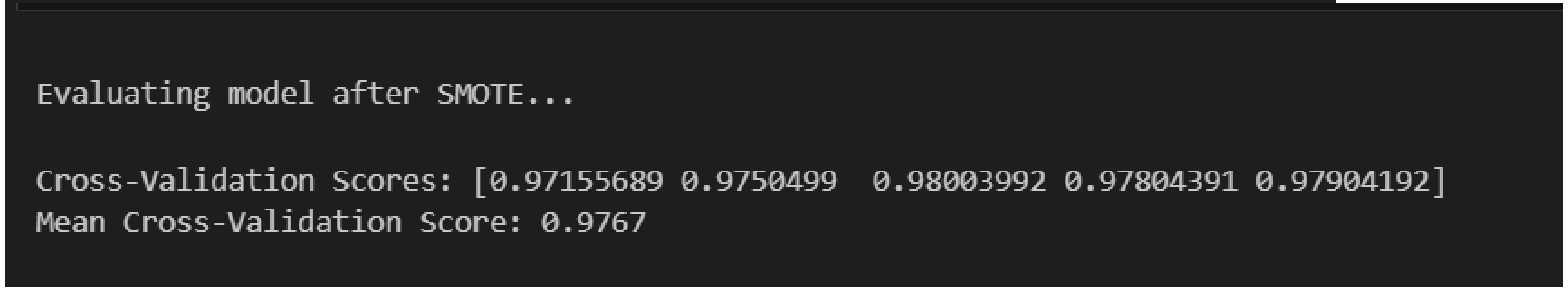


```
Evaluating model after SMOTE...

Cross-Validation Scores: [0.99550898 0.99700599 0.99850299 0.99850299 0.999002   ]
Mean Cross-Validation Score: 0.9977
```

Result of AB-RF on ECH Dataset

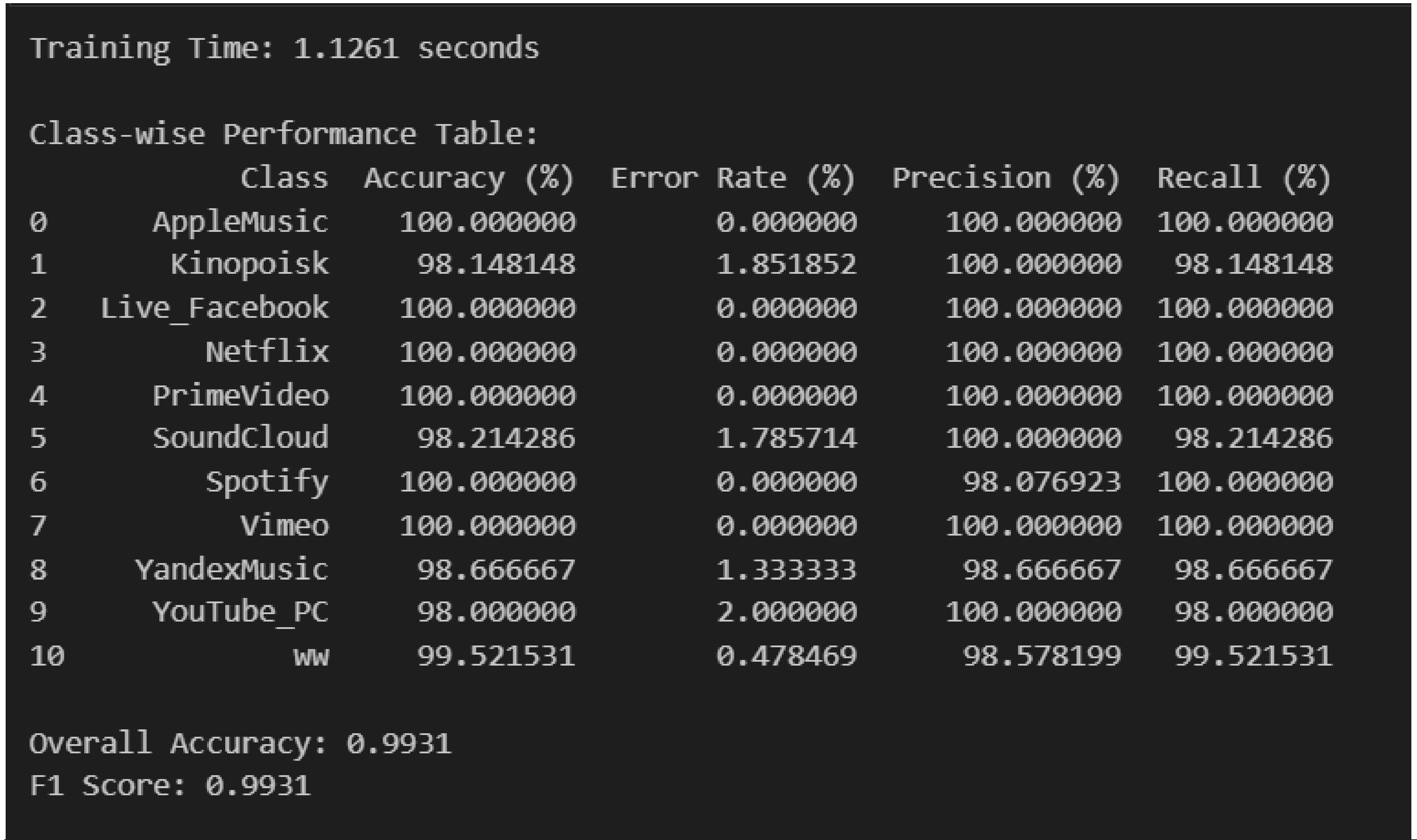


```
Training Time: 6.1302 seconds

Class-wise Performance Table:
            Class  Accuracy (%)  Error Rate (%)  Precision (%)  Recall (%)
0      AppleMusic    100.000000        0.000000      98.305085  100.000000
1       Kinopoisk     62.264151       37.735849      89.189189   62.264151
2   Live_Facebook    100.000000        0.000000     100.000000  100.000000
3    Live_Youtube    100.000000        0.000000     100.000000  100.000000
4         Netflix    100.000000        0.000000      78.703704  100.000000
5      PrimeVideo     86.842105       13.157895      89.189189   86.842105
6      SoundCloud    100.000000        0.000000      98.245614  100.000000
7         Spotify     98.000000        2.000000      87.500000   98.000000
8           Vimeo     73.684211       26.315789      87.500000   73.684211
9     YandexMusic     96.000000        4.000000      67.924528   96.000000
10     YouTube_PC    100.000000        0.000000     100.000000  100.000000
11             ww     76.960784       23.039216      96.913580   76.960784

Overall Accuracy: 0.8892
F1 Score: 0.8882
```

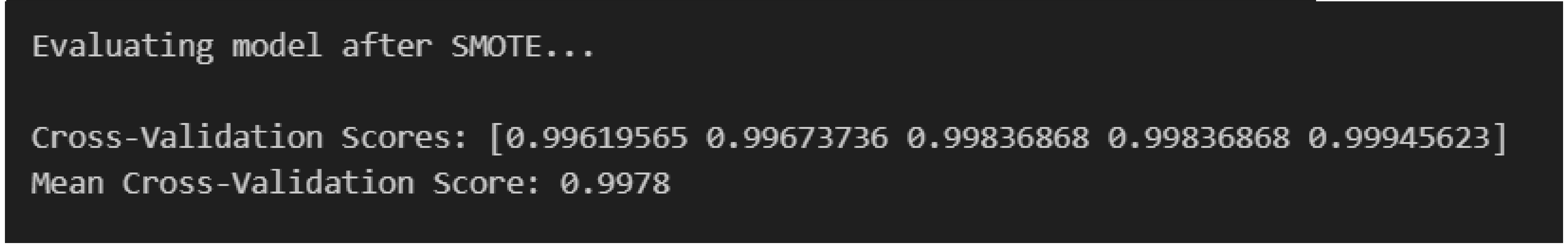


```
Evaluating model after SMOTE...

Cross-Validation Scores: [0.97155689 0.9750499  0.98003992 0.97804391 0.97904192]
Mean Cross-Validation Score: 0.9767
```

Result of RB-RF on ESNI Dataset

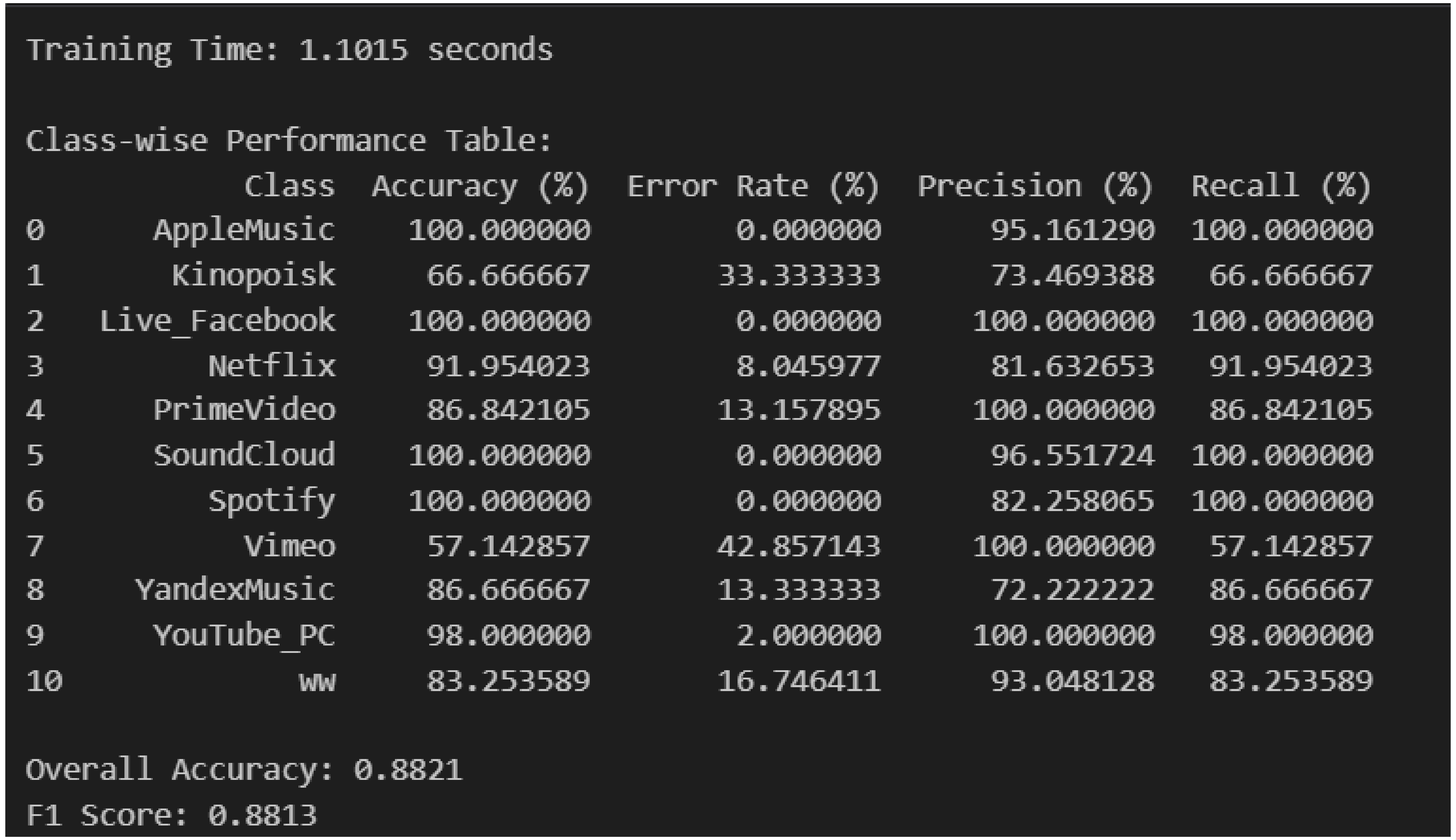


```
Training Time: 1.1261 seconds

Class-wise Performance Table:
            Class  Accuracy (%)  Error Rate (%)  Precision (%)  Recall (%)
0      AppleMusic    100.000000        0.000000     100.000000  100.000000
1       Kinopoisk     98.148148        1.851852     100.000000   98.148148
2   Live_Facebook    100.000000        0.000000     100.000000  100.000000
3         Netflix    100.000000        0.000000     100.000000  100.000000
4      PrimeVideo    100.000000        0.000000     100.000000  100.000000
5      SoundCloud     98.214286        1.785714     100.000000   98.214286
6         Spotify    100.000000        0.000000      98.076923  100.000000
7           Vimeo    100.000000        0.000000     100.000000  100.000000
8     YandexMusic     98.666667        1.333333      98.666667   98.666667
9      YouTube_PC     98.000000        2.000000     100.000000   98.000000
10             ww     99.521531        0.478469      98.578199   99.521531

Overall Accuracy: 0.9931
F1 Score: 0.9931
```

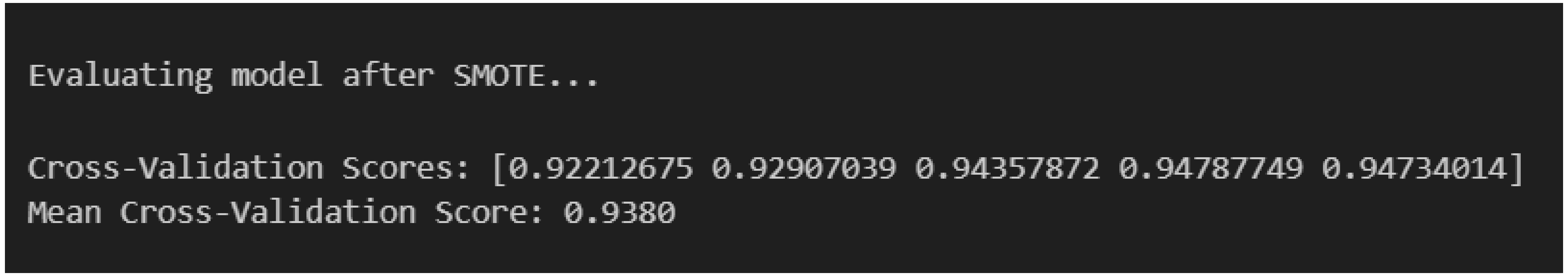


```
Evaluating model after SMOTE...

Cross-Validation Scores: [0.99619565 0.99673736 0.99836868 0.99836868 0.99945623]
Mean Cross-Validation Score: 0.9978
```

Result of RB-RF on ECH Dataset



```
Training Time: 1.1015 seconds

Class-wise Performance Table:
            Class  Accuracy (%)  Error Rate (%)  Precision (%)  Recall (%)
0      AppleMusic    100.000000        0.000000      95.161290  100.000000
1       Kinopoisk     66.666667       33.333333      73.469388   66.666667
2   Live_Facebook    100.000000        0.000000     100.000000  100.000000
3         Netflix     91.954023        8.045977      81.632653   91.954023
4       PrimeVideo     86.842105       13.157895     100.000000   86.842105
5      SoundCloud    100.000000        0.000000      96.551724  100.000000
6         Spotify    100.000000        0.000000      82.258065  100.000000
7           Vimeo     57.142857       42.857143     100.000000   57.142857
8     YandexMusic     86.666667       13.333333      72.222222   86.666667
9      YouTube_PC     98.000000        2.000000     100.000000   98.000000
10             ww     83.253589       16.746411      93.048128   83.253589

Overall Accuracy: 0.8821
F1 Score: 0.8813
```



```
Evaluating model after SMOTE...

Cross-Validation Scores: [0.92212675 0.92907039 0.94357872 0.94787749 0.94734014]
Mean Cross-Validation Score: 0.9380
```

Thank You