





# Classification of Simulated Fake Bandwidth Data Using LSTM

**Azriel Christian Nurcahyo** <sup>\*</sup>  
Design and Technology Centre,  
School of Computing and Creative  
Media, University of Technology  
Sarawak, 96000, Malaysia  
pic24030001@student.uts.edu.my  
*\*Corresponding author*

**Ting Huong Yong**   
Design and Technology Centre,  
School of Computing and Creative  
Media, University of Technology  
Sarawak, 96000, Malaysia  
alan.ting@uts.edu.my

**Abdulwahab Funsho Atanda**   
Design and Technology Centre,  
School of Computing and Creative  
Media, University of Technology  
Sarawak, 96000, Malaysia  
abdulwahab@uts.edu.my

 Submitted: 2024-08-17; Accepted: 2024-09-11; Published: 2024-09-21

**Abstract**— Hardly will someone acknowledge that the bandwidth we use every day is as authentic as most ISPs advertise, even those offering dedicated services. There are usually shortcomings, especially on upload and download bandwidth speeds. This paper presents the classification of simulated fake bandwidth data using the Long Short-Term Memory model, which though seldom found, is a very effective approach in network analysis. There were 1400 bandwidth data points collected from the MikroTik RB 1100 AHx device in a month, then further processed with normalization, and divided to have 80% training and 20% testing. The LSTM model applied had an accuracy rate of 98.93%, proving that it is capable of classifying either genuine or fake bandwidth instances accordingly. Of 1,400 test data points, the model managed to classify 723 as fake bandwidth and another 677 as genuine, resulting in a classification error rate of only 1.07%. The results clearly prove that LSTM has huge potential for real-time bandwidth manipulation detection, key to enhancing trust and efficiency in network management. In this respect, this research shows that bandwidth analysis combined with LSTM can be an original solution for network monitoring.

**Keywords**— Fake Bandwidth, LSTM, Data Classification

## I. INTRODUCTION

Bandwidth allocation integrity has been the paramount issue in the modern networking scene. This is because, nowadays, with internet service providers under increasing scrutiny for alleged practices of bandwidth manipulation to maximize their profit at the cost of customer experience, the situation has become critical (Varriale et al., 2024; Abbasloo, 2023; Jay et al., 2018). The issue of "fake bandwidth," where this happens due to an artificially inflated or throttled bandwidth measurement by an ISP, raises some serious ethical dilemmas about transparency and trust between the service provider and its customers in a network (Tilaye & Gojeh, 2020; Kim, 2014). This bandwidth manipulation, as a practice, can harm consumers directly because they do not receive the levels of internet service promised by the ISPs and undermine public confidence in the industry related to telecommunications (Azamuddin et al., 2020).

The term "fake bandwidth" refers to a situation whereby some Internet Service Providers willfully throttle or artificially inflate bandwidth measurements to cause customers the perception of faster Internet (The Drivers of Broadband Internet in Malaysia, 2023). This has become very controversial, involving heated debate within the telecommunications industries, regulatory bodies, and consumers at large. While this may just be a simple manipulation of algorithms for bandwidth management from an engineering point of view, it falls within the wider purview of ways an ISP can otherwise strip a customer of knowledge on network resources optimization (Said & Adham, 2015; Subektiningsih et al., 2022). The increasing number of consumer complaints about inconsistent internet speeds that is, advertisements at certain speeds are not always reflected in real-world performance has meant that various investigations and studies have been commissioned and conducted which reveal that some ISPs do have the ability to manipulate the reported bandwidth data (Dasmen & Khudri, 2021; Measuring Broadband America, 2023). It has evolved into a serious ethical issue, for it might directly hurt consumers who do not get the levels of internet service promised by the providers, and it could undermine faith in the industry within the psyche of the public (Li et al., 2019; MacMillan et al., 2022).

The fake bandwidth controversy has been receiving great attention of late following the emergence of high-profile cases in a number of countries. For example, investigations into some major ISPs in some developed countries have discovered that some were engaging in manipulation of the internet speeds they were offering customers (Redirecting DNS for Ads and Profit, 2023) (Mi et al., 2019) (Flach et al., 2016). Service providers, on the other hand, can reduce internet speed at times or regions to reduce their load, but still report a higher speed to customers due to bandwidth management that can still increase the ICMP and traffic sides (Bergman et al., 2018) (Balarezo et al., 2020) (Tilaye & Gojeh, 2020). This can be viewed as a lie to customers, for they are not accorded the services of internet levels they were promised, and this bandwidth manipulation practice can undermine public trust in the industry of telecommunications (Tilaye & Gojeh, 2020; Choffnes et al., 2017; Sait et al., 2016).

The artificial bandwidth problem is also a growing concern in Indonesia, where there is an increasing

dependence of the community on the internet for both business and personal needs (Budiman & Alam, 2017; Suryanegara et al., 2018; Antoni & Asvial, 2019; Dwiardi, 2020). Some Indonesian ISPs even have bandwidth manipulation practices, either by throttling internet speeds for specific applications or during certain periods, while simultaneously promoting consistent and advertised internet speeds to their subscribers (Bagus & Suryanegara, 2017; Indonesia WiFi Access Innovation, 2023; Aryotejo & Mufadhhol, 2019). This bandwidth throttling and misrepresentation practice is very questionable, as it harms customers in a straight line by not providing the level of internet services that were specified to them by the payment they have done, and further can undermine public trust in the whole telecommunications industry within the country itself (Measuring Fixed Broadband - Eighth Report, 2023; Bayat et al., 2022; & Dasmen, 2019).

The degree of bandwidth optimization taking place is what past research attempted to discover and quantify (Need, Want, Can Afford: Broadband Markets and the Behavior of Users, 2023; Anderson, 2013; Kim, 2014). Conversely, the outcome frequently emerges as controversial and provokes wider debate. Some studies have shown massive discrepancies between the reported internet speeds by the ISPs and actual real-world speeds faced by users, thus proving that ISPs are manipulating the bandwidth data reported (Feamster & Livingood, 2019; MacMillan et al., 2022; Mukti & Dasmen, 2019). Other studies, however, have demonstrated that these speed deviations can be triggered by a variety of legitimate technical factors, including distance from the distribution center or user device capacity, affecting the real internet speed experience of consumers (Pariag & Brecht, 2017; Nyarko-Boateng et al., 2019). This thereby progresses an ongoing debate in this area, underlining a clear requirement for more rigorous investigations so that the true cause of the discrepancies between advertised internet speeds and real-world speeds may be determined (Bauer et al., 2010; Capone et al., 2023).

This, however, is still an undeniable hot topic, more so considering the relevance of the internet that increases day by day today (Feamster & Livingood, 2019; Sharma et al., 2023). Transparency and reliability are what consumers are banking on from services they are paying for, and once consumers feel deceived by unethical practices in which bandwidth manipulation falls into, it can undermine their trust in ISPs (Massarczyk & Winzer, 2019). It is therefore upon this research to come up with better methods for detection and classification of fake bandwidth, which will help the consumers and regulators ensure that ISPs indeed provide services consistent with their promise (Zhou et al., 2018; Zhou et al., 2018).

In particular, it focuses on developing a high-accuracy classification model for the detection of fake bandwidth by using a Long Short-Term Memory network based on collected network activity data from MikroTik devices. Long Short Term Memory (LSTM) is a kind of RNN crafted to learn long-term dependencies (Yang et al., 2023; Donahue et al., 2015; Azzouni & Pujolle, 2017). An LSTM is one of the most interesting components of network

analysis, especially when dealing with sequential data for instance, network activities are normally temporal by nature. Another critical challenge regarding network analysis involves handling time-sequenced data where past information is critical in understanding future trends (Ribeiro et al., 2013; Saqr, 2023). LSTM operates with a unique mechanism, consisting of three main elements known as gates, the input gate, forget gate, and output gate (Yoon et al., 2023). The purpose of these gates is to manage the information flow, deciding which data to retain, eliminate, or utilize for producing an output. In contrast to traditional recurrent neural networks (RNNs), which frequently encounter difficulties related to the vanishing gradient issue, long short-term memory (LSTM) networks are adept at preserving pertinent information for extended durations. This characteristic renders LSTM particularly appropriate for network analyses that necessitate an understanding of temporal data patterns (Staudemeyer & Morris, 2019; Greff et al., 2017). LSTM can be used to detect anomaly patterns, predict network congestion, or even identify suspicious user behavior with high accuracy (Cheng et al., 2016; Karim et al., 2018; Sherstinsky, 2020). The ability of LSTMs to remember long-term information while predicting behavior extracted from sequences in data provides great value when modeling and analyzing bandwidth, data usage, or network flow optimization (Bi et al., 2022; Sherstinsky, 2020; Wang et al., 2021). It is able to detect patterns in the given dataset and is utilized for producing accurate forecasts or classification regarding network performance. The effectiveness of the LSTM would be higher, such that the detection of long-term patterns concerning network analysis has been achieved (Zhang et al., 2022; Bi et al., 2022). In contemporary network analysis, more sophisticated methodologies, such as the Long Short-Term Memory (LSTM) technique, are required (Sherstinsky, 2020; Tao et al., 2022). The conventional manual methods that are still prevalent among MikroTik users and network administrators are limited in their ability to fully exploit the available data (Macura et al., 2017; Song et al., 2020). Administrators typically concentrate on network monitoring through reactive approaches and static configurations, neglecting the fact that real-time data collection contains intricate and valuable information for prediction and optimization (D'Alconzo et al., 2019). By incorporating LSTM, network administrators can detect trends, potential congestion, or anomalies at an earlier stage, without relying on manual adjustments or reconfigurations that may disrupt operations (Lu & Yang, 2018; Ye et al., 2022). This approach facilitates the transition from reactive to proactive management, paving the way for future network transformation, while ensuring optimal performance without adding strain to the existing infrastructure. The vast potential of collected network data remains untapped without methodologies like LSTM, hindering the full utilization of network efficiency and reliability, which has been a persistent challenge thus far (Waczyńska et al., 2021; Casas, 2020). Exploiting the power of deep learning and real-world availability of network data, this work adds to the efforts in progress

toward rectifying manipulations on bandwidth and the eventual restoration of faith in the telecommunications industry.

## II. RESEARCH METHODS

### A. Network Design Model

Beginning from a default reset on the MikroTik router, a new admin password was input, and then the network interface was configured with CLI scripting. The WAN connects the LAN to the Internet and requires a public IP address from the ISP to this model of router. This would act as the internal network to which all client devices would connect; the IP addresses used can be /16 and /24. Secondly, it must have a DHCP server that should be enabled, which would provide the connected computers with an IP address automatically between 192.168.20.1 and 192.168.21.253. This would be two IP segments to use more IPs. Second, NAT and routing configurations are done. Masquerade NAT is applied on the WAN interface to save on public IPs. Remote access is allowed via OpenVPN for easier remote control. The OpenVPN server scripting is as follows:

```
client
dev tun
proto tcp
remote id-17.hostddns.us 1194
resolv-retry infinite
nobind
route-method exe
persist-key
persist-tun
remote-cert-tls server
cipher AES-128-CBC
auth SHA1
auth-user-pass pass.txt
verb 2
<ca>
-----BEGIN CERTIFICATE-----
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxx
-----END CERTIFICATE-----
</ca>
```

Meanwhile, on the RB 1100 AHx router, the OpenVPN configuration can be set up as follows:

```
/interface ovpn-client add connect-
to=id-17.hostddns.us name=
pic24030001@student.uts.edu.my
password=xxxxxxx user=
pic24030001@student.uts.edu.my
comment=id-17.hostddns.us:5010<->23
```

Static routing is also configured to route traffic from the local network to the ISP and to correctly assign all paths, so that there is proper allocation for local access, high-bandwidth access, and access to local servers. A firewall is then established, this blocks all types of traffic coming into the system from an external source, except for pre-defined established and related connections. That way, data packets as part of an ongoing connection still can cross through the firewall. Moreover, it allows DNS and DHCP to pass through, so the network can run without interruptions. Two techniques are used for easy data retrieval, namely, using the syslog daemon to obtain log data and active control through the Kid Control feature. This feature offers real-time monitoring of internet activities over IP and MAC addresses. Logging for all events of access control enforcement is enabled when Kid Control rules are applied. It will retain the logs on the RB 1100 AHx in this case since it has enormous storage. Further, every action, in real-time, shall be captured by these logs, which are also integrated with a syslog daemon. The next step was to gather and collect data from the Kid Control logs. First, a simulation was made wherein data points of around 120 were gathered in one day for training. The actual research work followed afterwards with a larger scale of log gathering that concluded with the collection of up to 7,000 bandwidth data points to be used for further analysis. The results from data collection are validated, after which it is followed by LSTM classification. In a situation where the data collection is invalid or not as expected, troubleshooting is carried out through the steps of Kid Control by repeating the collection until satisfying results are achieved, making it involve download and upload activities, IP addresses, connections, activity access. The step-by-step flowchart model used in this research can be seen in figure 1 as follows

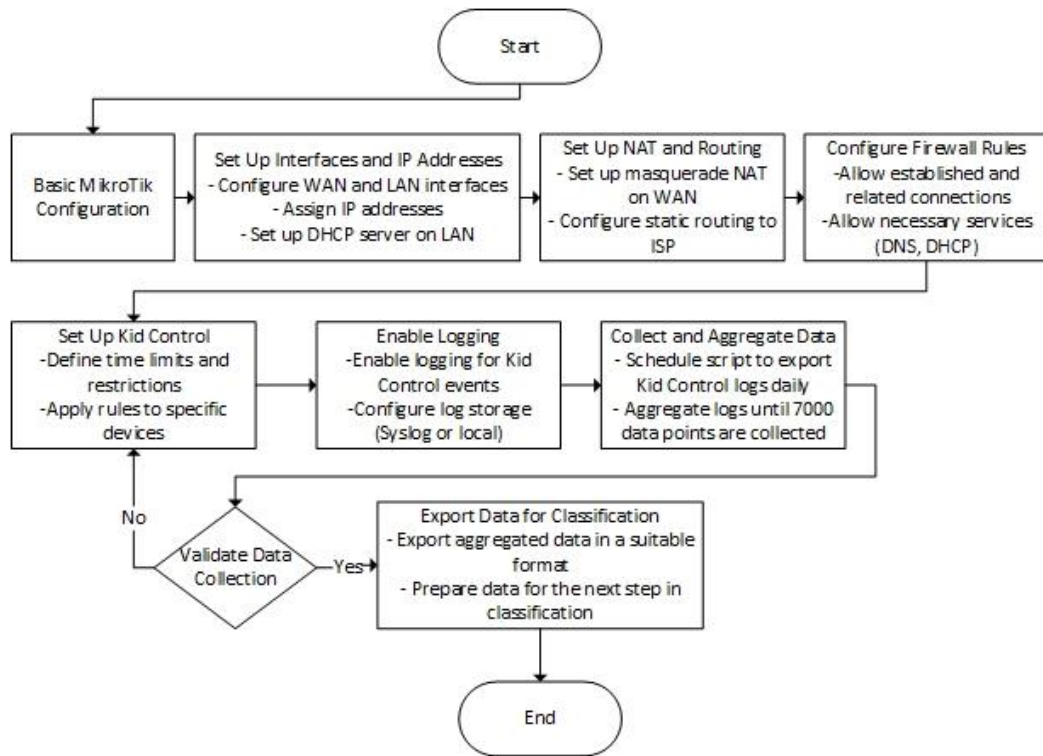


Figure 1. Network Model Flowchart Used

At the data link layer, every device has a MAC address that serves as its unique identifier. Information in relation to the details of the users that have accessed this network creates metadata with very vital contextual information, enabling linking between usage patterns and user identities tied to it. Whether statically or dynamically configured using DHCP, the IP address acts as a logical address for the network layer. It provides efficient routing of data packets to and from devices. This IP address does not merely provide a destination for the arriving packets but also identifies the source and outbound data paths that, in turn, are used to optimize routes and analyze network loads at various points.

Subsequently, the data is collected in the form of rate-up and rate-down bandwidth metrics, which account for the actual throughput at the transport layer. This sort of data may be used to build granular views into how network capacity is being consumed and provide direct indicators of potential congestion, bottlenecks, or bandwidth use, as shown in Figure 2. Moreover, bytes up bandwidth and bytes down bandwidth show the volume of data that is transmitted and received, which forms the critical metric in management bandwidth allocation, capacity planning, and enforcing fair usage policies by quota or service prioritization in heavy quota based or service priority networks.

Action	IP Address	Rate Up	Rate Down	Bytes Up	Bytes Down	Activity
OPPO A45	192.168.20.191	86 Mbps	4.5 Mbps	46.624.225	787.715 KB	www.facebook.com
Galaxy S20	192.168.20.192	107 Mbps	175.5 Mbps	506.026.256	1.021.926.742	youtube.com
Pixel 6	192.168.20.193	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.194	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.195	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.196	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.197	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.198	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.199	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.200	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.201	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.202	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.203	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.204	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.205	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.206	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.207	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.208	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.209	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.210	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.211	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.212	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.213	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.214	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.215	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.216	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.217	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.218	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.219	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.220	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.221	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.222	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.223	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.224	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.225	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.226	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.227	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.228	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.229	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.230	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.231	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.232	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.233	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.234	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.235	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.236	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.237	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.238	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.239	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.240	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.241	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.242	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.243	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.244	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.245	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.246	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.247	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.248	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.249	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.250	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.251	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.252	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.253	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.254	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com
Pixel 6	192.168.20.255	107 Mbps	107 Mbps	906.026.256	906.026.256	www.youtube.com

Figure 2. Data Log Collection of Activity and Bandwidth on RB 1100 Ahx

Activity logs, therefore, track certain activities concerning access to websites or network services that come in handy with detailed data concerning the behavior of the users within the network for the visited sites. This data will be fully used to determine what bandwidth is genuine and which ones are fake depending on the data collected. The captured image of the bandwidth management model in this research can be seen in Figure 3, and the network configuration consisting of the main backbone router, core switch, and manageable switches that are integrated for this study can be seen in Figure 4.

Avg. Rate	Queued Bytes	Bytes	Packets
35.5 kbps	0 B	3133.2 MiB	10 516 849
1881.5 kbps	0 B	654.4 GiB	625 029 188
60.9 kbps	0 B	177.7 GiB	181 815 721
60.9 kbps	0 B	177.7 GiB	181 815 721
0 bps	0 B	0 B	0
0 bps	0 B	0 B	0
240 bps	0 B	49.6 GiB	45 280 928
240 bps	0 B	49.6 GiB	45 280 928
1820.3 kbps	0 B	427.1 GiB	397 932 539
1820.3 kbps	0 B	427.1 GiB	397 932 539
261.3 kbps	0 B	88.8 GiB	408 645 380
36.1 kbps	0 B	26.9 GiB	138 230 590
36.1 kbps	0 B	26.9 GiB	138 230 590
0 bps	0 B	0 B	0
0 bps	0 B	0 B	0
0 bps	0 B	4659.6 MiB	30 035 258
0 bps	0 B	4659.6 MiB	30 035 258
225.2 kbps	0 B	57.3 GiB	240 379 532
225.2 kbps	0 B	57.3 GiB	240 379 532

Figure 3. Bandwidth Management Results on RB 1100



Figure 4. MikroTik Backbone Used (Router Number 2 RB 1100 AHx)

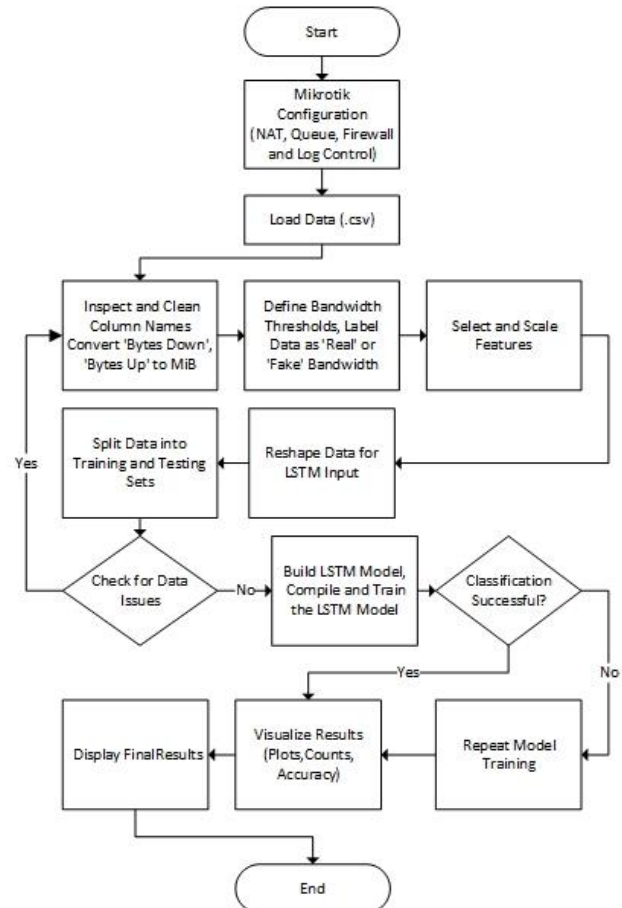


Figure 5. LSTM Implementation Model

### B. LSTM Implementation

The Python coding process is carried out on Google Colab with a csv dataset that was retrieved from the MikroTik configuration. First, NAT, Queue, Firewall, and Log Control must be set up so that network devices will be able to track and monitor data traffic effectively. As illustrated in figure 5, import the .csv file containing recorded network data for analysis. Figure 5 illustrates the bandwidth classification process using the LSTM model.

First, it verifies the consistency of column names in the imported dataset. Second, cleaning columns converting Bytes Down and Bytes Up into units of MiB for ease of processing. It assumes the size of data may appear in any format, either KiB, MiB, GiB, or TiB, and is hence changed into MiB using a simple conversion formula. For example, if it's in KiB, the value will be divided by 1024 to convert it into MiB. Similarly, for GiB and TiB, values shall be multiplied by factors of 1024 or 1024<sup>2</sup>.

The next step is to set the bandwidth threshold for the classification of the data. This threshold is determined from the expected bandwidth speeds, that are 15 Mbps download and 10 Mbps upload. These numbers, 15 and 10, are the managed bandwidth for download and upload on the MikroTik RB 1100 Ahx, used by 50 users simultaneously for a period of one month. The speeds are converted into MiB from bits per second, with 1 byte taken as equal to 8 bits. Download speed of 15 Mbps is converted as  $15 \times 1024^2 / 8$ , which comes to around 1.788 MiB per second for download. The upload speed of 10 Mbps is converted as  $10 \times 1024^2 / 8$ , which comes to around 1.19 MiB per second for upload.

After defining the thresholds, data is labeled as Real Bandwidth in cases where bytes\_down\_mib equals or is more than 1.788 MiB/second and bytes\_up\_mib equals or is more than 1.19 MiB/second, otherwise it would be Fake Bandwidth. The next step is to make feature selection and standardization of those selected features. In this study, bytes\_down\_mib and bytes\_up\_mib are both normalized



with a Min Max Scaler, which embeds these values in the range between 0 and 1 so that data is uniformly scaled. This normalization is important to be performed so that the LSTM model could learn well without suffering from the large discrepancies of scales of features.

After standardization, the data is reshaped in a particular manner to be fed into the LSTM model. This prepares the data into a 3D format [samples, timesteps, number of features]. Given that this model uses just one timestep, the data becomes [n\_samples, 1, 2], where 2 refers to two features that are used bytes\_down\_mib and bytes\_up\_mib. Data is split into two parts: 80% as training data and 20% as testing data. The split is random, which will avoid the possibility for the model to try to fit some data points and let it generalize well with unseen data.

The LSTM model has been architected with three different LSTM layers. The first layer has 100 units, so return\_sequences = true allows information contained in sequences to pass to the next layers. The second contains 100 units, return\_sequences = true, continuing the learning of sequences. The third is composed of 50 units with the end of sequences without return\_sequences, which marks the end of the processing of LSTM sequences. Every LSTM layer is followed by a dropout layer, a method used to create multiple different models: randomly shut off some neurons in the layer during training to avoid overfitting. This is followed by two dense layers after the LSTM layers with the final layer having a SoftMax activation function, classifying the data into two different categories Real Bandwidth or Fake Bandwidth.

Following this, the model is compiled with the Adam optimizer, a learning rate of 0.001, and the categorical cross entropy loss function since this is a multi-class classification transformed into one hot encoding. The model will be trained over 50 epochs with a batch size of 64, and validation during training was performed on the test data. Finally, testing is done on the testing dataset after training. For every class, a probabilistic prediction is computed, and the final predicted labels are determined based on the argmax of the predicted probabilities. A confusion matrix is then used for the estimation of the model performance, showing the number of correct and wrong predictions, and a classification report, which presents detailed metrics for each class, such as precision, recall, and the F1-score.

It was also constructed with a receiver operating characteristic curve to assess the proficiency of the model in class separation by computing the Area Under the Curve. This would mean that the higher the AUC value, the better the model at discriminating classes of Real Bandwidth and Fake Bandwidth.

In results visualization, multiple plots were generated. The first set of graphs shows the loss and accuracy during the training process, which describes how the model is learning and how well it is doing on both the training and test data. Plotting the ROC curve shows how well the model classifies. It will further be used to visualize the Real and Fake Bandwidth distributions of data on, respectively, bytes\_down\_mib and bytes\_up\_mib features. A bar plot could show the count of classifications for each

class. The final visualization will be a 3D scatter plot of the data in bytes\_down\_mib versus bytes\_up\_mib, with their corresponding labels. This graph provides a visualization perspective on how data is spread inside a three-dimensional space. The accuracy of the model will be given as a percentage of correct predictions on the test data, with other metrics that give assessment of how well the model is at classifying.

### C. Sample Data Simulation

Before carrying out the holistic process of data collection, a one-day simulation was conducted that returned 114 valid data, where classification between real and fake bandwidth was done mathematically by extracting features, transforming the data, and processing sequential data using a Long Short-Term Memory neural network. It worked on a dataset containing MAC address, IP address, network activity, and bytes downloaded and uploaded. Key features for this process were bytes\_down\_mib and bytes\_up\_mib. These features are of major use during this process, which has been converted into megabytes per second from their original format in MiB. This was done through a function, whereby each value of the data, either measured in KiB, MiB, GiB, or TiB, was standardized for further analysis. The data was then converted, and the next operation was checking if the data obtained met the threshold of the real bandwidth. Real bandwidth was based on a standard of 15 Mbps for download and 10 Mbps for upload, converted to 1.875 MiB/s download and 1.25 MiB/s upload. Any value above the threshold values is therefore considered Real Bandwidth, and the rest, Fake Bandwidth. These labels were used as targets in the model training process. In this simulation, there is an LSTM with a depth of two LSTM layers and two dropout layers for overfitting prevention. The model was created to discover a pattern in the data that would mean real or fake bandwidth usage.

This processed data was then transformed into sequences so that they can be fed into the LSTM model, where every example was represented as a sequence containing the features bytes\_down\_mib and bytes\_up\_mib. The model was trained for 30 epochs using the Adam optimization algorithm and the binary cross entropy loss function. The result of this training returned an accuracy of 77.19% against the validation data. Confusion matrix analysis showed that only fake bandwidth was identified with full accuracy, real bandwidth was not detected at all. The detailed results of the classification simulation test distinguishing between fake bandwidth and real bandwidth, using sample data prior to the analysis of the actual 30-day data, are presented in Table 1.

Table 1. Simulation Results, Classification Report

	Precision	Recall	F1-score	Support
0	0.77	1.00	0.87	88
1	0.00	0.00	0.00	26
Accuracy			0.77	114
Macro Avg	0.39	0.50	0.44	114
Weighted Avg	0.60	0.77	0.67	114

This is a confusion matrix where 114 test data points had the model correct in classifying 88 instances as false bandwidth but failed to identify a single example from the data points that were of real bandwidth. The graph in Figure 6 is a monotonically decreasing loss on the training data, which therefore shows that the model has learnt from the data.

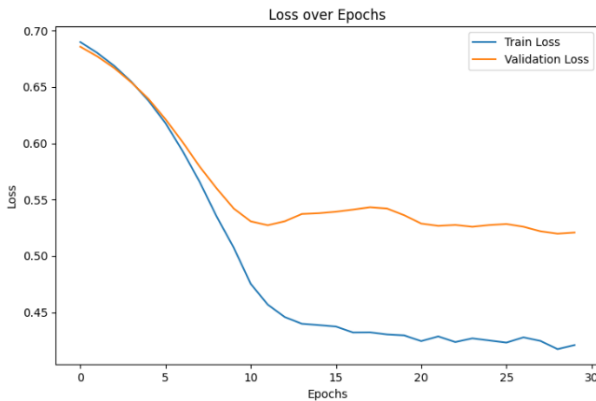


Figure 6. Loss over Epochs for Network Sample Data

Since this loss is decreasing during training, it means this model becomes better at capturing the underlying pattern of the training dataset. The validation loss, however, shows a near stationarity trend, indicating that improvements in model performance on the training data do not exactly transfer to the validation set. This plateauing of the validation loss may indicate that the model is reaching its capacity to generalize from the training dataset to the unseen data in figure 7. Probably, the process of overfitting had started, or further tuning of hyperparameters might be required for better generalization.

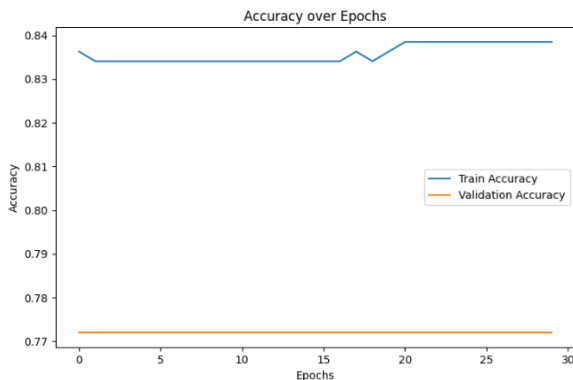


Figure 7. Accuracy over Epochs for Network Sample Data

The model did improve its accuracy during the training. One can see from the graph that training accuracy tended to stabilize at about 84% while validation accuracy remained almost the same at 77.19%. That means it was hard for this model to generalize more unseen data, very likely due to the small size of the dataset and class imbalance.

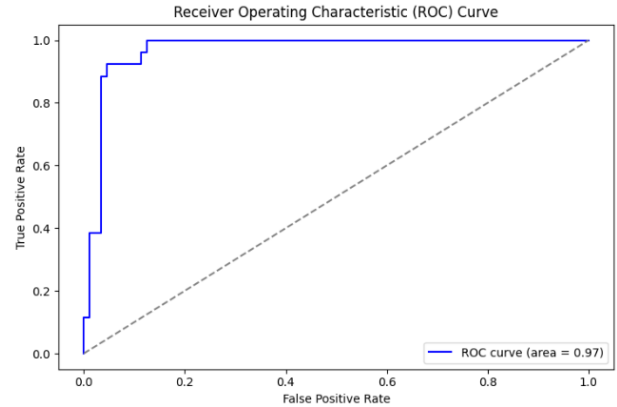


Figure 8. ROC Curve for the Sample Network Data

The ROC curve in figure 8 is a graph showing model performance based on this trade off of TPR versus FPR. Based on the area under the curve value of 0.97, the ROC curve highlights how much potential the model has to distinguish between these two classes effectively but has not been in a position to realize this completely on this smaller test dataset mainly because it is poor at generating positive predictions. The results of the classification report provide details of the metrics in terms of precision, recall, and f1-score for each class. It is clearly represented that precision and recall for True Bandwidth are zero, therefore showing this model has completely failed to detect True Bandwidth but has great results while detecting Fake Bandwidth as shown in the final sample data results in Table 2 for the Confusion Matrix.

Table 2. Simulation Results, Confusion Matrix

Confusion Matrix	Predicted	Predicted
	False	True
Actual False	88	0
Actual True	26	0
Test Accuracy	77.19%	

### III. RESULT AND DISCUSSION

#### A. Network Configuration Results

Therefore, the ether1 interface is perfectly managed by configuring the bandwidth to the figures recorded with real data for one month from July 10, 2024, to August 10, 2024, within the system log. Such figures are proven by what is shown in the download throughput Rx, which reaches up to 10.3 Mbps, and in the upload Tx, which stabilizes at 1329.0 kbps. These metrics show that the system can keep up a high and stable download speed that is consistent with the queue configuration put in place. Figure 9 presents the graph depicting the performance of the ether1 interface, which was connected to the internet gateway and

distributed to more than 1000 users on the network using RB 1100 AHx, operating continuously for 30 days without interruption.

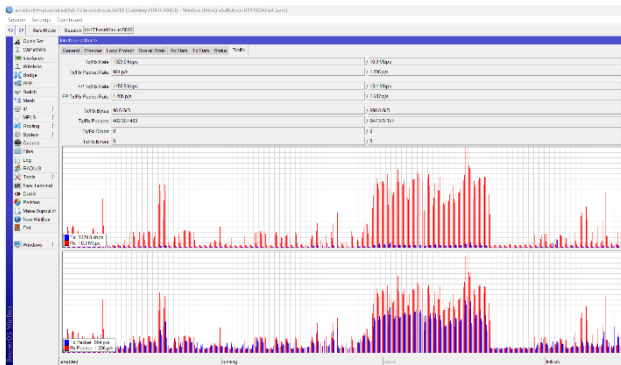


Figure 9. Network Monitoring Graph for Ether 1 on MikroTik

The volume of data transferred across the network is very large, and the Tx/Rx Bytes, so far recorded, come to 96.5 GiB for transmitter data and 690.8 GiB for received data. These figures underline how busy the network has been, which is represented in the traffic graph as a function of time and changes/variability in bandwidth use. These variations are thus highly relevant indicators of network performance and capacity and illustrate peaks of heavy usage and troughs of light activity that are important in terms of optimizing traffic management and load balancing.

The Tx/Rx Packets metric, which represents the total of data packets processed, was 402,307,483 for Tx Packets and 647,375,157 for Rx Packets. This high count of packets demonstrates the large volume of data transactions going on within the network, hence a strong and well-used network infrastructure. Tx/Rx Drops remained at zero, further confirming the efficiency of data transmission processes. No data packets were lost during transit, which is very critical to data integrity and reliable communication over the network.

System logs from Kid Control and Sys Daemon Log generated detailed logs of activities of every connected device, capturing such vital metrics as data volume and transfer speed. These logs represent a rich dataset, primed for further analysis using an LSTM model in the domain of deep learning. Helped by this model, the system can then spot subtle patterns in bandwidth usage, thus classifying real and fake bandwidth from a dataset of 1400 records.

### B. Results of the LSTM-Based Fake Bandwidth Testing

Integration of the simulation test results, and classification of bandwidth data provides the basis for an in-depth discussion on the way a deep learning-based system, empowered with the architecture of Long Short-Term Memory (LSTM) networks, impeccably works in distinguishing between real (Real Bandwidth) and fake (Fake Bandwidth) bandwidth. This advanced process commences with step-by-step preprocessing of the

uploaded data, which includes some network activity metrics such as bytes\_down, bytes\_up, and ancillary data in the face of user browsing behavior, IP addresses, and MAC addresses. Systematically, raw data is converted to ensure consistency across the dataset and ease of computations into bytes\_down and bytes\_up columns, representing the data in MiB (Mebibytes) in a standardized form.

The LSTM model used for this simulation is multilayered. The three LSTM layers have different numbers of neurons, and smartly implemented Dropout layers help to prevent overfitting of the model. The model is trained on a preprocessed dataset, which consists of 1400 data points. Further breaking down this dataset, 80% of the data has been used for training and the remaining 20% for testing the model's efficiency. The outcomes of this categorization are then graphed accordingly using several more sophisticated visual illustrations, for example, scatterplot along with a 3D scatter plot to come up with a representation of the distribution of genuine and fake bandwidth data based on the measurement of bytes\_down and bytes\_up. This can be observed in the results shown in figure 10 for the scatter plot and figure 11 for the 3D visualization model in detail. This advanced analytical approach shows the robustness of the LSTM architecture in processing sequenced input data characterizing network traffic, thus enabling it to learn hidden representations of the patterns distinguishing real bandwidth use cases from the ones potentially manipulated. The deployment of such a model not only enhances our understanding of bandwidth allocation but also offers a potent tool for real time monitoring of the network and fraud detection.

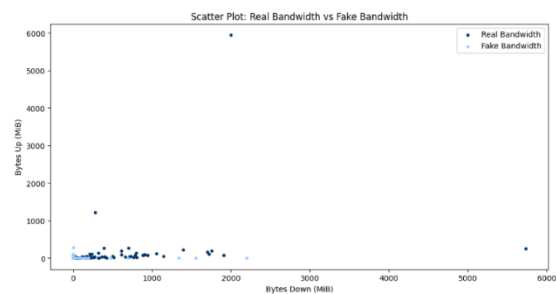


Figure 10. Scatter Plot for Fake and Real Bandwidth



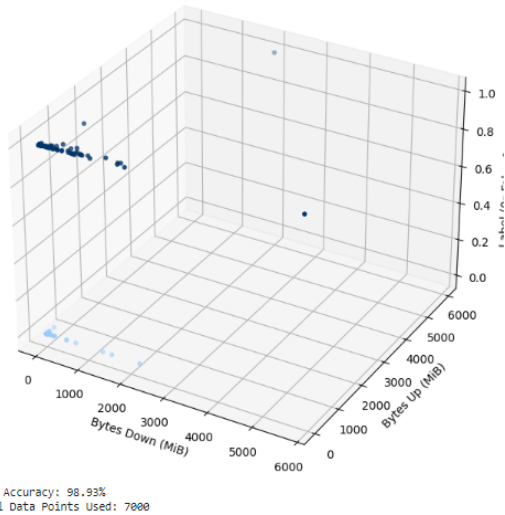


Figure 11. 3D Visualization Model of Fake and Real Bandwidth

Scatter plots show that the real bandwidth data, on average, is concentrated either in the center or in a specific area of the graph, whereas the fake bandwidth data is scattered, clearly highlighting the gap between the two categories. As shown in the Confusion Matrix, which was obtained from the testing phase, the model’s accuracy is 98.93%, which is very high and hence excellent. Out of 1400 test data points, the model correctly classified 708 instances of fake bandwidth and 677 instances of real bandwidth. Only 15 data points were misclassified, underscoring how well the model performed in differentiating between genuine and counterfeit bandwidth data. This evidence can be seen in figure 12.

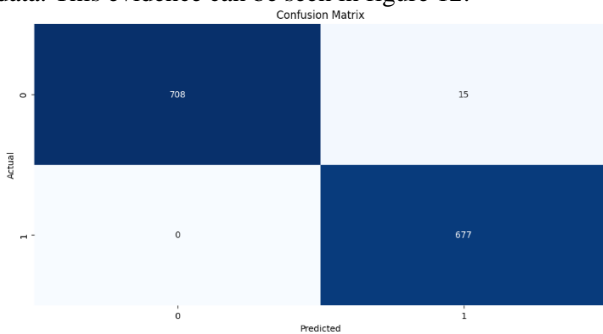


Figure 12. Confusion Matrix Result

It is quite evident from the Classification Report that the model performed with very high precision and high recall values close to 1.00 for both classes, such as real and fake bandwidth. This looks like the description of a highly accurate model in predicting the correct class, yet very consistent in making sure it reduced classification errors. This performance underlines the model’s robustness and reliability to efficiently recognize either category of bandwidth, hence with minimal false classifications. This is reflected in the data shown in Tables 3 and 4, which indicate nearly perfect results for accuracy and F1 score.

Table 3. Fake Bandwidth Confusion Matrix

Confusion Matrix	Predicted False	Predicted True
Actual False	708	15
Actual True	0	677
<b>Test Accuracy</b>	<b>98.93%</b>	

Table 4. Fake Bandwidth Classification Report

	Precision	Recall	F1-score	Support
Fake B.	1.00	0.98	0.99	723
Real B.	0.98	1.00	0.99	677
Accuracy			0.99	1400
Macro Avg	0.99	0.99	0.99	1400
Weighted Avg	0.99	0.99	0.99	1400

These results indicate that, all things considered, from the 1,400 test data points, the distribution between the real and fake bandwidth remained fairly balanced. However, the LSTM model used showed quite a good ability to ensure great delineation between the two classes. This would, therefore, prove that the LSTM technique is very well suited for the task of classifying bandwidth data of this nature. Thus, the performance of the model is an indication that it can be effectively applied further on implementation in real-time network monitoring and management. That the LSTM model can differentiate accurately between genuine and manipulated bandwidth data means it may turn out to be very useful in enhancing network security measures and bandwidth allocation optimization. Therefore, this is a very vital tool in maintaining integrity and efficiency in network operations. This evidence can be seen in the Loss over Epochs (LSTM) in Figure 13, the Accuracy over Epochs (LSTM) in Figure 14, and the Results of the ROC Curve shown in Figure 15.

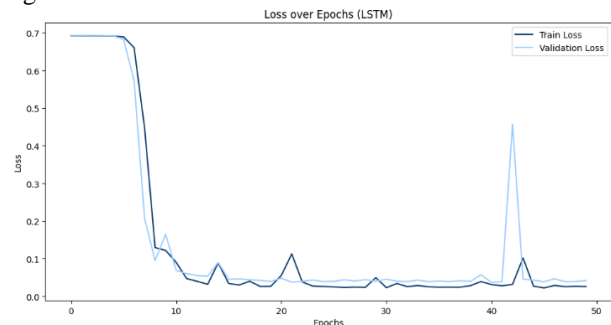


Figure 13. Results of Loss over Epochs (LSTM)

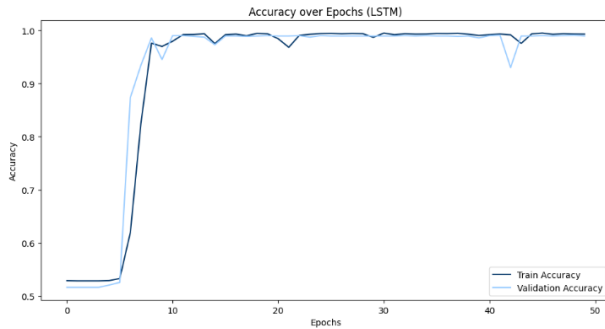


Figure 14. Results of Accuracy over Epochs (LSTM)

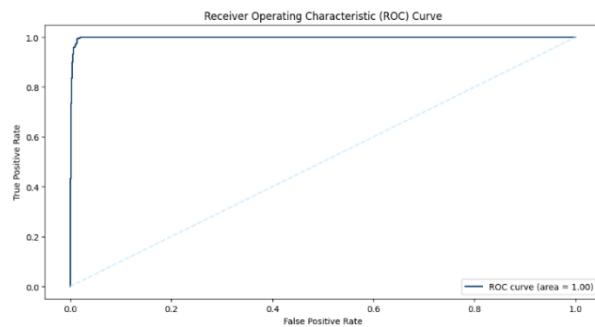


Figure 15. Results of the ROC Curve

Out of the test set of 1,400 samples, 708 samples of fake bandwidth and 677 samples of actual bandwidth were correctly predicted as True Negatives and True Positives, respectively. Fifteen real bandwidth samples were misclassified as fake, i.e., False Positives, and no fake samples of bandwidth were detected as real, i.e., False Negatives. Thus, the precision for fake bandwidth is 1.00, meaning all predictions of fake bandwidth were true. The recall for fake bandwidth is 0.98, meaning the model was almost perfect in the identification of fake bandwidth. The precision for real bandwidth is equal to 0.98, consequently indicating some slight mistakes in the correct identification of real bandwidth.

The model rapidly reached a high level of accuracy after about the first 10 epochs and then remained stable at around 98-99% until the end. This goes to show that the model very fast learned the patterns necessary to distinguish between classes and maintained this without significant overfitting, as given by the consistency between training and validation accuracy. The graph of loss demonstrates a sharp real drop in the values of the loss in the first period of training, then the line flattens out, which corresponds to stable model performance in making the right predictions of classes.

Mathematically, the model brings down both Type I and Type II errors and proves to be very robust in handling imbalanced classes. High precision and recall of the metrics further underline the effectiveness of the LSTM architecture at capturing temporal dependencies and sequential patterns intrinsic to bandwidth data. The fact that it also performs consistently accurately on the validation data and is independent of training set significantly justifies the generalization ability of the model, thereby making it a very strong tool suited for real-

time network management applications where bandwidth classification is required.

### C. Model Performance And Classification Results

In the case of this study, real bandwidth is defined as a condition wherein bytes\_down and bytes\_up, which are amount of data downloaded and uploaded respectively, are greater than predefined thresholds (15 Mbps for download and 10 Mbps for upload). Data that does not meet these criteria are classed as fake bandwidth. The LSTM model implemented for this work is relatively complex in the sense that it comprises several LSTM layers, each of which goes with a Dropout layer to avoid overfitting. For training this model, a dataset was divided into two parts: 80% of the database was used for training and 20% for testing.

Throughout more than 50 epochs, the model increased its accuracy dramatically to eventually provide an accuracy of 98.93%. This result proves that the model learned the pattern in data well and could differentiate between real and fake bandwidth. A confusion matrix, which is always output for the performance of a model in test data, has shown that out of 1,400 test samples, 708 instances of fake bandwidth were correctly classified, and 677 instances of real bandwidth were rightly identified. This came about with just 15 classification errors all on the fake bandwidth. No error was made on the real bandwidth. Such an outcome would suggest that the model precision and recall are both very close to 1.00 hence, very accurate and consistent. Mathematically, these results mean that out of the 1,400 data points being tested, nearly all the data classed as fake bandwidth actually met the initial criteria for classification to a very high degree of accuracy. Just 15 of the 1,400 test data points were misclassified as fake bandwidth, giving a very low error proportion of about 1.07%. This result therefore clearly shows that the system is very good and reliable at recognizing anomalies in bandwidth.

## IV. CONCLUSION

Out of the 1,400 measured data points, the model correctly classified 723 of the instances as either fake bandwidth and 677 of them as real bandwidth instances. This suggests a kind of compromise between real and fake bandwidth over the course of a month, thereby proving the efficiency of the LSTM model on network data preprocessed by the RB 1100 AHx router. Such high accuracy and analysis confirm the effectiveness of the LSTM model in distinguishing between the bandwidth that is real and that which is fake, hence securing the network monitoring efficiently. Through numerical data and graphical results, the presented case of the reliability of the model for this task of classification is presented with a very low error rate. This means that more important analysis should be made under different data models other than a single big network model the likes concerning user access patterns or bandwidth usage patterns across multiple routers. Such could ensure the robustness and adaptability of the LSTM model in varied network environments.

## ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to all those who contributed, particularly to the Design and Technology Centre, School of Computing and Creative Media, University of Technology Sarawak, and to the School of Postgraduate Studies, University of Technology Sarawak.

## REFERENCES

- Abbasloo, S. (2023, January 1). Internet Congestion Control Benchmarking. *Cornell University*. <https://doi.org/10.48550/arxiv.2307.10054>
- Anderson, C. (2013, January 1). Dimming the Internet: Detecting Throttling as a Mechanism of Censorship in Iran. *Cornell University*. <https://doi.org/10.48550/arxiv.1306.4361>
- Antoni, Y., & Asvial, M. (2019, June 1). Strategy of National Fiber Optic Backbone Network Utilization Enhancement in Rural Area of Indonesia. *IEEE International Conference on Information and Communication Technology for Rural Development (ICIRD)*, 9074750. <https://doi.org/10.1109/icird47319.2019.9074750>
- Aryotejo, G., & Mufadhol, M. (2019, May 1). Static and dynamic alliance: the solution of reliable internet bandwidth management. *IOP Conference Series: Materials Science and Engineering*, 1217(1), 012126-012126. <https://doi.org/10.1088/1742-6596/1217/1/012126>
- Azamuddin, W. M. H., Hassan, R., Aman, A. H. M., Hasan, M. K., & Al-Khaleefa, A. S. (2020, May 12). Quality of Service (QoS) Management for Local Area Network (LAN) Using Traffic Policy Technique to Secure Congestion. *Multidisciplinary Digital Publishing Institute*, 9(2), 39-39. <https://doi.org/10.3390/computers9020039>
- Azzouni, A., & Pujolle, G. (2017, January 1). A Long Short-Term Memory Recurrent Neural Network Framework for Network Traffic Matrix Prediction. *Cornell University*. <https://doi.org/10.48550/arXiv.1705>
- Bagus, R., & Suryanegara, M. (2017, August 1). Network management models to anticipate the problem of international Internet traffic in Indonesia. *IEEE International Seminar on Intelligent Technology and Its Applications (ISITIA)*, 8124047. <https://doi.org/10.1109/isitia.2017.8124047>
- Balarezo, J. F., Wang, S., Gomez, K., Al-Hourani, A., Fu, J., & Kandeepan, S. (2020, December 14). Low-rate TCP DDoS Attack Model in the Southbound Channel of Software Defined Networks. *IEEE International Conference on Signal Processing and Communication Systems (ICSPCS)*, 9310040. <https://doi.org/10.1109/icspcs50536.2020.9310040>
- Bauer, S., Clark, D. D., & Lehr, W. (2010, August 15). Understanding Broadband Speed Measurements. *RELX Group (Netherlands)*. [http://cfp.mit.edu/events/may11/CFP%20Spring%202011%20PDFs/Bauer\\_Clark\\_Lehr\\_Broadband\\_Speed\\_Measurements.pdf](http://cfp.mit.edu/events/may11/CFP%20Spring%202011%20PDFs/Bauer_Clark_Lehr_Broadband_Speed_Measurements.pdf)
- Bayat, N., Misra, V., & Rubenstein, D. (2022, January 1). Bandwidth Allocation Games. *Cornell University*. <https://doi.org/10.48550/arXiv.2204>
- Bi, J., Zhang, X., Yuan, H., Zhang, J., & Zhou, M. (2022, July 1). A Hybrid Prediction Method for Realistic Network Traffic With Temporal Convolutional Network and LSTM. *Institute of Electrical and Electronics Engineers*, 19(3), 1869-1879. <https://doi.org/10.1109/tase.2021.3077537>
- Budiman, E., & Alam, S. N. (2017, November 1). User perceptions of mobile internet services performance in borneo. *International Association for Cryptologic Research*, 8280643. <https://doi.org/10.1109/iac.2017.8280643>
- Capone, A., Dècina, M., Milan, A., & Petracca, M. (2023, January 1). Modelling the Performance of High Capacity Access Networks for the Benefit of End-Users and Public Policies. *Cornell University*. <https://doi.org/10.48550/arXiv.2305>
- Casas, P. (2020, January 1). Two Decades of AI4NETS-AI/ML for Data Networks: Challenges & Research Directions. *Cornell University*. <https://doi.org/10.48550/arxiv.2003.04080>
- Cheng, M., Xu, Q., L.V., J., Wenyin, L., Li, Q., & Wang, J. (2016, November 1). MS-LSTM: A multi-scale LSTM model for BGP anomaly detection. <https://doi.org/10.1109/icnp.2016.7785326>
- Choffnes, D., Gill, P., & Mislove, A. (2017, March 27). An Empirical Evaluation of Deployed DPI Middleboxes and Their Implications for Policymakers. *Social Science Research Network*. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2941535](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941535)
- D'Alconzo, A., Drago, I., Morichetta, A., Mellia, M., & Casas, P. (2019, September 1). A Survey on Big Data for Network Traffic Monitoring and Analysis. *Institute of Electrical and Electronics Engineers*, 16(3), 800-813. <https://doi.org/10.1109/tnsm.2019.2933358>
- Dasmen, R. N., & Khudri, A. (2021, February 9). Optimasi Jaringan Wireless PT. TASPEN dengan RADIUS Server dan Firewall Filter Rules. *Jurnal Teknik Komputer*, 20(1), 134-146. <https://doi.org/10.33633/tc.v20i1.4183>
- Donahue, J., Hendricks, L. A., Guadarrama, S., Rohrbach, M., Venugopalan, S., Darrell, T., & Saenko, K. (2015, June 1). Long-term recurrent convolutional networks for visual recognition and description. <https://doi.org/10.1109/cvpr.2015.7298878>
- Dwiardi, A. R. (2020, October 1). Analysis of the Needs of ICT Ecosystems to Support the Acceleration of Internet Fixed Broadband Penetration (case: Bogor, Sumedang, Bangli, and Karangasem). *Journal of Information Systems and Informatics (JSI)*, 10(1), 41-58. <https://doi.org/10.17933/jppi.v10i1.298>
- Feamster, N., & Livingood, J. (2019, January 1). Internet Speed Measurement: Current Challenges and Future

- Recommendations. *Cornell University*. <https://doi.org/10.48550/arxiv.1905.02334>
- Flach, T., Papageorge, P., Terzis, A., Pedrosa, L., Cheng, Y., Karim, T., Katz-Bassett, E., & Govindan, R. (2016, August 22). An Internet-Wide Analysis of Traffic Policing. *ACM SIGCOMM Computer Communication Review*, 2934873. <https://doi.org/10.1145/2934872.2934873>
- Greff, K., Srivastava, R. K., Koutnik, J., Steunebrink, B. R., & Schmidhuber, J. (2017, October 1). LSTM: A Search Space Odyssey. *Institute of Electrical and Electronics Engineers*, 28(10), 2222-2232. <https://doi.org/10.1109/tnnls.2016.2582924>
- Indonesia WiFi Access Innovation. (2023, February 6). *Web Archive*. <https://web.archive.org/web/20100507222442/http://lirneasia.net/projects/2004-05/indonesia-wifi/>
- Jay, N., Rotman, N. H., Godfrey, P. B., Schapira, M., & Tamar, A. (2018, January 1). Internet Congestion Control via Deep Reinforcement Learning. *Cornell University*. <https://doi.org/10.48550/arxiv.1810.03259>
- Karim, F., Majumdar, S., Darabi, H., & Chen, S. (2018, January 1). LSTM Fully Convolutional Networks for Time Series Classification. *Institute of Electrical and Electronics Engineers*, 6, 1662-1669. <https://doi.org/10.1109/access.2017.2779939>
- Kim, K. S. (2014, January 1). Toward Fully-Shared Access: Designing ISP Service Plans Leveraging Excess Bandwidth Allocation. *Cornell University*. <https://doi.org/10.48550/arxiv.1409.4499>
- Li, F., Niaki, A. A., Choffnes, D., Gill, P., & Mislove, A. (2019, August 19). A large-scale analysis of deployed traffic differentiation practices. *Proceedings of the ACM SIGCOMM Conference*, 3341302. <https://doi.org/10.1145/3341302.3342092>
- Lu, H., & Yang, F. (2018, December 1). Research on Network Traffic Prediction Based on Long Short-Term Memory Neural Network. <https://doi.org/10.1109/compcomm.2018.8781071>
- MacMillan, K., Mangla, T., Saxon, J., Marwell, N. P., & Feamster, N. (2022, January 1). A Comparative Analysis of Ookla Speedtest and Measurement Labs Network Diagnostic Test (NDT7). *Cornell University*. <https://doi.org/10.48550/arxiv.2205.12376>
- Macura, L., Rozhon, J., & Lin, J. C. (2017, November 2). Employing Monitoring System to Analyze Incidents in Computer Network. <https://doi.org/10.5772/intechopen.71102>
- Massarczyk, R., & Winzer, P. J. (2019, July 1). Influence of the Perceived Data Security, Credibility, Trust and Confidence on the Usage Frequency of Internet Services and the Provision of Security Measures. *SPECTS 2019: Proceedings of the 2019 International Symposium on Performance Evaluation of Computer and Telecommunication Systems*, 8823527. <https://doi.org/10.23919/spects.2019.8823527>
- Measuring Broadband America. (2023, February 22). *Federal Communications Commission*. <https://www.fcc.gov/reports-research/reports/measuring-broadband-america/measuring-broadband-america-july-2012>
- Measuring Fixed Broadband - Eighth Report. (2023, February 6). *Federal Communications Commission*. <https://www.fcc.gov/reports-research/reports/measuring-broadband-america/measuring-fixed-broadband-eighth-report>
- Mi, X., Feng, X., Liao, X., Liu, B., Wang, X., Qian, F., Li, Z., Alrwais, S., Sun, L., & Liu, Y. (2019, May 1). Resident Evil: Understanding Residential IP Proxy as a Dark Service. *Proceedings of the IEEE Symposium on Security and Privacy*, 00011. <https://doi.org/10.1109/sp.2019.00011>
- Mukti, A. R., & Dasmen, R. N. (2019, May 30). Prototipe Manajemen Bandwidth pada Jaringan Internet Hotel Harvani dengan Mikrotik RB 750r2. *Jurnal Penelitian Ilmu Teknik (JPIT)*, 4(2), 87-92. <https://doi.org/10.30591/jpit.v4i2.1322>
- Nyarko-Boateng, O., Adekoya, A. F., & Weyori, B. A. (2019, March 1). Investigating QoS and Performance of Received Signal Strength Indicator in Fiber Optics Broadband Data Communication. *American Journal of Engineering and Applied Sciences*, 12(3), 391-401. <https://doi.org/10.3844/ajeassp.2019.391.401>
- Pariag, D., & Brecht, T. (2017, January 1). Application Bandwidth and Flow Rates from 3 Trillion Flows Across 45 Carrier Networks. *Springer Science+Business Media*, 129-141. [https://doi.org/10.1007/978-3-319-54328-4\\_10](https://doi.org/10.1007/978-3-319-54328-4_10)
- Ramayah, S. N. L. U. S. M. P. M. R. T. U. S. M. P. M. (2023, November 10). The Drivers of Broadband Internet in Malaysia. *IEEE Xplore*. <https://ieeexplore.ieee.org/document/7808315/>
- Redirecting DNS for Ads and Profit. (2023, January 7). *International Computer Science Institute, Berkeley*. <https://www.icsi.berkeley.edu/pubs/networking/redirectingdnsforads11.pdf>
- Ribeiro, B., Perra, N., & Baronchelli, A. (2013, October 21). Quantifying the effect of temporal resolution on time-varying networks. *Nature Portfolio*, 3(1). <https://doi.org/10.1038/srep03006>
- Sait, S. Y., Murthy, H. A., & Sivalingam, K. M. (2016, November 1). Organization-Level Control of Excessive Internet Downloads. *IEEE Local Computer Network Conference (LCN)*, 38. <https://doi.org/10.1109/lcn.2016.38>
- Saqr, M. (2023, January 1). Temporal network analysis: Introduction, methods and detailed tutorial with R. *Cornell University*. <https://doi.org/10.48550/arxiv.2307.12339>
- Sharma, R., Richardson, M., Martins, G., & Feamster, N. (2023, January 1). Measuring the Prevalence of WiFi Bottlenecks in Home Access Networks. *Cornell University*. <https://doi.org/10.48550/arxiv.2311.05499>

- Sherstinsky, A. (2020, March 1). Fundamentals of Recurrent Neural Network (RNN) and Long Short-Term Memory (LSTM) network. *Elsevier BV*, 404, 132306-132306. <https://doi.org/10.1016/j.physd.2019.132306>
- Song, W., Beshley, M., Przystupa, K., Beshley, H., Кочан, O., Pryslupskyi, A., Pieniak, D., & Su, J. (2020, March 14). A Software Deep Packet Inspection System for Network Traffic Analysis and Anomaly Detection. *Multidisciplinary Digital Publishing Institute*, 20(6), 1637-1637. <https://doi.org/10.3390/s20061637>
- Stanojevic, Z. S. B. F. E. B. R. (2023, November 10). Need, Want, Can Afford: Broadband Markets and the Behavior of Users. *ACM Digital Library*. <https://dl.acm.org/doi/10.1145/2663716.2663753>
- Staudemeyer, R. C., & Morris, E. R. (2019, January 1). Understanding LSTM -- a tutorial into Long Short-Term Memory Recurrent Neural Networks. *Cornell University*. <https://doi.org/10.48550/arxiv.1909.09586>
- Subektiningsih, S., Renaldi, R., & Ferdiansyah, P. (2022, January 1). Analisis Perbandingan Parameter QoS Standar TIPHON Pada Jaringan Nirkabel Dalam Penerapan Metode PCQ. *Explore: Jurnal Penelitian dan Pengembangan IPTEK*, 12(1), 57-57. <https://doi.org/10.35200/explore.v12i1.527>
- Suryanegara, M., Andriyanto, F., & Arifin, A. S. (2018, June 1). Lessons Learned from the Quality of Experience (QoE) Assessment of 4G Mobile Technology in Indonesia. *Institute of Advanced Engineering and Science (IAES)*, 10(3), 1203-1203. <https://doi.org/10.11591/ijeecs.v10.i3.pp1203-1211>
- Tao, J., Sun, B., Zhu, W., Qu, S., Lingkun, C., Li, J., Li, G., Chong, W., Xiong, Y., & Zhou, J. (2022, January 1). The Deep learning model of upstream and downstream brain regions Based on Memory Generation-Consolidation-Loss, Synaptic Strength Rebalance and mnemonic spiral. *Cornell University*. <https://doi.org/10.48550/arXiv.2203>
- Tilaye, G., & Gojeh, L. A. (2020, January 1). Use of Access Control List Application for Bandwidth Management among Selected Public Higher Education Institutions in Ethiopia. *Computers in Science and Technology*, 8(1), 24-35. <https://doi.org/10.13189/csit.2020.080103>
- Varriale, V., Cammarano, A., Michelino, F., & Caputo, M. (2024, June 1). The role of digital technologies in production systems for achieving sustainable development goals. *Elsevier BV*, 47, 87-104. <https://doi.org/10.1016/j.spc.2024.03.035>
- Waczyńska, J., Martelli, E., Vallecorsa, S., Karavakis, E., & Cass, T. (2021, January 1). Convolutional LSTM models to estimate network traffic. *EDP Sciences*, 251, 02050-02050. <https://doi.org/10.1051/epjconf/202125102050>
- Wang, Y., Gui, G., Gacanin, H., Ohtsuki, T., Dobre, O. A., & Poor, H. V. (2021, August 1). An Efficient Specific Emitter Identification Method Based on Complex-Valued Neural Networks and Network Compression. Yang, F., Liu, J., Zhang, R., & Yang, F. (2023, May 15). Diffusion characteristics classification framework for identification of diffusion source in complex networks. *Public Library of Science*, 18(5), e0285563-e0285563. <https://doi.org/10.1371/journal.pone.0285563>
- Ye, Y., Wang, Y., Liao, J., Chen, J., Zou, Y., Liu, Y., & Feng, C. (2022, July 22). Spatiotemporal Pattern Analysis of Land Use Functions in Contiguous Coastal Cities Based on Long-Term Time Series Remote Sensing Data: A Case Study of Bohai Sea Region, China. *Multidisciplinary Digital Publishing Institute*, 14(15), 3518-3518. <https://doi.org/10.3390/rs14153518>
- Yoon, S., Kim, M., & Lee, W. (2023, January 1). Long Short-Term Memory-Based Deep Learning Models for Screening Parkinson's Disease Using Sequential Diagnostic Codes. *Journal of Clinical Neurology*, 19(3), 270-270. <https://doi.org/10.3988/jcn.2022.0160>
- Zhang, X., Zhang, R., & Wang, X. (2022, November 14). Visual SLAM Mapping Based on YOLOv5 in Dynamic Scenes. *Multidisciplinary Digital Publishing Institute*, 12(22), 11548-11548. <https://doi.org/10.3390/app122211548>
- Zhou, P., Chang, R. K. C., Gu, X., Fei, M., & Zhou, J. (2018, January 1). Magic Train: Design of Measurement Methods against Bandwidth Inflation Attacks. *IEEE Transactions on Dependable and Secure Computing*, 15(1), 98-111. <https://doi.org/10.1109/tdsc.2015.2509984>