

**TINGKAT KEAMANAN JARINGAN HOME WI-FI DI KOTA  
YOGYAKARTA TERHADAP PASSWORD ATTACK**

**TUGAS AKHIR**



**PANGGIH GUMELARING PRAJA**

**NIM 20106050046**

**STATE ISLAMIC UNIVERSITY  
SUNAN KALIJAGA  
YOGYAKARTA**

**PROGRAM STUDI INFORMATIKA**

**FAKULTAS SAINS DAN TEKNOLOGI**

**UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA**

**YOGYAKARTA**

**2024**

# HALAMAN PENGESAHAN



KEMENTERIAN AGAMA  
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA  
FAKULTAS SAINS DAN TEKNOLOGI  
Jl. Marsda Adisucipto Telp. (0274) 540971 Fax. (0274) 519739 Yogyakarta 55281

## PENGESAHAN TUGAS AKHIR

Nomor : B-801/Un.02/DST/PP.00.9/06/2024

Tugas Akhir dengan judul : TINGKAT KEAMANAN JARINGAN HOME WI-FI DI KOTA YOGYAKARTA  
TERHADAP PASSWORD ATTACK

yang dipersiapkan dan disusun oleh:

Nama : PANGGIH GUMELARING PRAJA  
Nomor Induk Mahasiswa : 20106050046  
Telah diujikan pada : Kamis, 30 Mei 2024  
Nilai ujian Tugas Akhir : A

dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta

### TIM UJIAN TUGAS AKHIR



Ketua Sidang  
Ir. Muhammad Taufiq Nuruzzaman, S.T. M.Eng., Ph.D.  
SIGNED

Valid ID: 665d1acc768d6



Penguji I  
Dr. Ir. Bambang Sugiantoro, S.Si., M.T.,  
IPM., ASEAN Eng.  
SIGNED

Valid ID: 665aa62715feb



Penguji II  
Mandahadi Kusuma, M.Eng.  
SIGNED

Valid ID: 66596fa454aa2



Yogyakarta, 30 Mei 2024  
UIN Sunan Kalijaga  
Dekan Fakultas Sains dan Teknologi  
Prof. Dr. Dra. Hj. Khurul Wardati, M.Si.  
SIGNED

Valid ID: 665d54de26aa6

## LEMBAR PERNYATAAN

### LEMBAR PERNYATAAN

Yang bertanda tangan di bawah ini:

Nama : Panggih Gumelaring Praja

NIM : 20106050046

Dosen Pembimbing : Ir. Muhammad Taufiq Nuruzzaman, S.T., M.Eng., Ph.D.

Menyatakan bahwa skripsi saya yang berjudul "**Tingkat Keamanan Jaringan Home Wi-Fi di Kota Yogyakarta Terhadap Password Attack**" adalah hasil penelitian saya sendiri. Sejauh yang saya tahu, penelitian yang saya lakukan ini belum pernah dilakukan atau diterbitkan di tempat lain terkecuali perihal acuan atau kutipan pada daftar pustaka yang tertulis dalam naskah ini. Selain itu, skripsi ini juga diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Informatika pada Fakultas Sains dan Teknologi, Universitas Islam Negeri Sunan Kalijaga Yogyakarta.

Yogyakarta, 20 Mei 2024

Yang menyatakan,



Panggih Gumelaring Praja

NIM 20106050046

STATE ISLAMIC UNIVERSITY  
SUNAN KALIJAGA  
YOGYAKARTA

## SURAT PERSETUJUAN SKRIPSI



KEMENTERIAN AGAMA  
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA  
FAKULTAS SAINS DAN TEKNOLOGI  
Jl. Marsda Adisucipto Telp. (0274) 515856 Yogyakarta 55281

### SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal : Persetujuan Skripsi

Lamp : -

Kepada

Yth. Dekan Fakultas Sains dan Teknologi  
UIN Sunan Kalijaga Yogyakarta  
di Yogyakarta

*Assalamualaikum Wr. Wb.*

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka kami selaku pembimbing berpendapat bahwa skripsi Saudara:

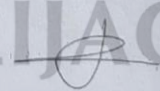
Nama : Pangih Gumelaring Praja  
NIM : 20106050046  
Judul Skripsi : Tingkat Keamanan Jaringan *Home* Wi-Fi di Kota  
Yogyakarta terhadap *Password Attack*

sudah dapat diajukan kembali kepada Program Studi Informatika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu dalam Program Studi Informatika.

Dengan ini kami mengharap agar skripsi/tugas akhir Saudara dapat segera di-*munaqasyah*-kan. Atas perhatiannya kami ucapkan terima kasih.

*Wassalamualaikum Wr. Wb.*

Yogyakarta, 22 April 2024  
Pembimbing,

  
Ir. M Taufiq N, S.T. M.Eng., Ph.D.  
NIP. 19791118 200501 1 003

## MOTTO

“Diwajibkan atas kamu berperang, padahal itu kamu benci. Boleh jadi kamu membenci sesuatu, padahal itu baik bagimu dan boleh jadi kamu menyukai sesuatu, padahal itu buruk bagimu. Allah mengetahui, sedangkan kamu tidak mengetahui”

### Q.S. Al-Baqoroh: 216

Apakah kamu akan membenci seorang dokter yang telah membunuh beberapa orang karena kebaikan hatinya?

*“You only live once, but if you do it right, once is enough”*

**Stephen King**

“Hal besar sejauh ini adalah menjadi metafora; itu adalah satu hal yang tidak dapat dipelajari dari orang lain dan itu juga merupakan tanda kejeniusan, karena metafora yang baik menyiratkan persepsi intuitif tentang kesamaan dari yang berbeda”

**Aristoteles**

*“Homo proponit, sed Deus disponit”*

Manusia berencana, Tuhan memutuskan



## HALAMAN PERSEMBAHAN

*Bissmillahirrahmaanirrahiim*, atas karunia-Nya skripsi ini penulis persembahkan kepada:

**Rusmono, SE. dan Sainah**

Selaku orang tua tercinta sekaligus sosok inspirasi dan alasan semua ini terlaksana dengan baik

**Lina Fuji Lestari, SE., Panji Trisula, S.IP., dan Prakas Pringgajati**

Selaku kakak dan adik tersayang

**Semua pihak yang terlibat baik saudara, teman-teman seperjuangan,  
maupun dosen**

Yang selalu memberikan dukungan dan arahan untuk penulis

Dan

**Almamater tercinta**

**Program Studi Informatika**

**Fakultas Sains dan Teknologi**

**UIN Sunan Kalijaga Yogyakarta**

## **LEMBAR PEDOMAN PENGGUNAAN TUGAS AKHIR**

*Tugas Akhir ini tidak dipublikasikan, tetapi tersedia di perpustakaan dalam lingkungan UIN Sunan Kalijaga Yogyakarta, diperkenankan dipakai sebagai referensi kepustakaan, tetapi pengutipan harus seizin penyusun, dan harus menyebutkan sumbernya sesuai dengan kebiasaan ilmiah. Dokumen Tugas Akhir ini merupakan hak milik UIN Sunan Kalijaga Yogyakarta.*



## ABSTRAK

Penggunaan teknologi Wi-Fi yang meningkat seiring berjalannya waktu menimbulkan keresahan dikarenakan masalah keamanan jaringan yang masih mendapat sedikit perhatian. Kota Yogyakarta sebagai penyandang kota dengan indeks literasi digital tertinggi dan perencanaan program *smart city*-nya belum ada jaminan keamanan terkait permasalahan ini.

Penelitian ini ditunjukan untuk mengkaji tingkat keamanan jaringan *home Wi-Fi* terhadap *password attack* untuk keperluan data statistik dan bahan edukasi. Metode pengambilan sampel yang digunakan yaitu teknik *quota sampling* dan *penetration testing* sebagai metode pengumpulan datanya.

Hasil penelitian menunjukkan serangan *WPA cracking* dan *WPS cracking* berhasil mendapatkan sebagian kecil akses *login* berupa *password* serta mengukur persentase keamanan tingkat kota maupun di setiap kecamatannya. Selain data serangan, terdapat beberapa rekomendasi untuk melindungi *access point* supaya terhindar dari serangan tersebut.

**Kata kunci:** Wi-Fi, *password attack*, *WPA cracking*, *WPS cracking*





## KATA PENGANTAR

*Assalamu'alaikum* Wr. Wb.

*Alhamdulillah* *rabbil'alamin*, segala puji dan syukur penulis panjatkan kehadirat Allah SWT yang telah memberikan rahmat dan hidayah-Nya sehingga skripsi dengan judul “Tingkat Keamanan Jaringan *Home* Wi-Fi di Kota Yogyakarta terhadap *Password Attack*” ini bisa diselesaikan tepat waktu. Skripsi ini hadir sebagai tugas akhir perkuliahan serta persyaratan untuk memperoleh gelar Sarjana Strata 1 Program Studi Informatika Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta.

Melalui penelitian ini, penulis berharap kontribusi ilmiah yang dilakukan dapat memberikan manfaat bagi perkembangan ilmu pengetahuan dan praktik khususnya dalam bidang informatika/teknologi. Skripsi ini juga bisa selesai atas bimbingan, arahan, masukan, serta dukungan dari berbagai pihak. Oleh karena itu, penulis mengucapkan terima kasih sebanyak-banyaknya kepada:

1. Bapak Prof. Dr. Phil. Al Makin, S.Ag., MA., selaku Rektor Universitas Islam Negeri Sunan Kalijaga Yogyakarta.
2. Ibu Prof. Dr. Dra. Hj. Khurul Wardati, M.Si., selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta.
3. Ibu Maria Ulfah Siregar, S.Kom., MIT., Ph.D. selaku Ketua Program Studi Informatika Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta.
4. Bapak Mandahadi Kusuma, M.Eng. selaku Dosen Pembimbing Akademik yang telah membarengi serta memberikan informasi selama perkuliahan.
5. Bapak Ir. Muhammad Taufiq Nuruzzaman, S.T., M.Eng., Ph.D. selaku Dosen Pembimbing Skripsi yang telah meluangkan waktunya untuk mengarahkan dan mengevaluasi selama proses skripsi.
6. Orang tua saya tercinta, H. Rusmono, SE. dan Hj. Sainah yang selalu memberikan kasih sayang, nasehat, dan doa untuk keberhasilan serta kelancaran anakmu ini.

7. Kakak-kakak saya, Lina Fuji Lestari, SE. dan Panji Trisula, S.IP., serta adik saya Prakas Pringgajati yang telah memberikan dukungan berupa motivasi maupun dukungan material.
8. Seluruh Masjid di Kota Yogyakarta yang telah menjadi tempat singgah untuk pengambilan data, tempat istirahat, dan tempat beribadah selama penelitian dilakukan.
9. Teman saya, Ismail (Butak) yang selalu ada untuk diajak mancing bersama untuk menghilangkan stres selama proses pembuatan skripsi.
10. Teman-teman seperjuangan, Informatika angkatan 2020 Universitas Islam Negeri Sunan Kalijaga Yogyakarta.
11. Semua pihak yang telah membantu dalam penyusunan skripsi yang tidak bisa disebutkan satu persatu.

Penulis berharap semoga dukungan serta kontribusi yang diberikan oleh pihak terkait mendapatkan balasan dari Allah SWT dan penelitian ini dapat bermanfaat bagi kita semua.

*Wassalamu'alaikum* Wr. Wb.

Yogyakarta, 15 Mei 2024

Penyusun,

STATE ISLAMIC UNIVERSITY  
SUNAN KALIJAGA  
YOGYAKARTA  
Panggih Gumelaring Praja  
NIM 20106050046

## DAFTAR ISI

HALAMAN PENGESAHAN.....	ii
LEMBAR PERNYATAAN .....	iii
SURAT PERSETUJUAN SKRIPSI.....	iv
MOTTO.....	v
HALAMAN PERSEMBAHAN .....	vi
LEMBAR PEDOMAN PENGGUNAAN TUGAS AKHIR.....	vii
ABSTRAK .....	viii
KATA PENGANTAR.....	ix
DAFTAR ISI .....	xi
DAFTAR TABEL.....	xiii
DAFTAR GAMBAR .....	xiv
DAFTAR LAMPIRAN .....	xv
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang .....	1
1.2 Rumusan Masalah .....	3
1.3 Batasan Masalah.....	3
1.4 Tujuan Penelitian.....	4
1.5 Manfaat Penelitian.....	5
BAB II TINJAUAN PUSTAKA DAN LANDASAN TEORI.....	6
2.1 Tinjauan Pustaka.....	6
2.2 Landasan Teori .....	12
2.2.1 Pengertian Jaringan <i>Wireless</i> .....	12
2.2.2 Jenis-jenis Jaringan <i>Wireless</i> .....	12

2.2.3	Konsep Keamanan Jaringan.....	14
2.2.4	Metode Keamanan Protokol WLAN.....	17
2.2.5	WLAN <i>Hacking</i> .....	19
BAB III METODE PENELITIAN.....		22
3.1	Waktu dan Tempat Penelitian.....	22
3.2	Alat dan Bahan Penelitian.....	22
3.2.1	Alat.....	22
3.2.2	Bahan.....	22
3.3	Metode Penelitian.....	23
3.3.1	Populasi Penelitian.....	23
3.3.2	Sampel Penelitian.....	23
3.3.3	Metode Pengumpulan Data.....	26
BAB IV HASIL DAN PEMBAHASAN.....		29
4.1	<i>Penetration Testing</i> .....	29
4.2	Hasil Pengujian Keamanan <i>Home Wi-Fi</i> .....	33
4.3	<i>Wi-Fi Protected Access (WPA) Cracking</i> .....	37
4.4	<i>Wi-Fi Protected Setup (WPS) Cracking</i> .....	41
4.5	Solusi Pengamanan.....	44
BAB V PENUTUP.....		50
5.1	Kesimpulan.....	50
5.2	Saran.....	50
DAFTAR PUSTAKA.....		52

## DAFTAR TABEL

Tabel 2.1 Ringkasan Tinjauan Pustaka .....	9
Tabel 3.1 Jumlah Sampel Penelitian .....	25
Tabel 4.1 Sampel Data Hasil Penelitian.....	34
Tabel 4.2 Jumlah Total Serangan .....	36
Tabel 4.3 Persentase Keamanan Per-Kecamatan .....	36
Tabel 4.4 Sampel Data Serangan WPA <i>Cracking</i> .....	38
Tabel 4.5 Data Serangan Berhasil WPA <i>Cracking</i> .....	40
Tabel 4.6 Sampel Data Serangan WPS <i>Cracking</i> .....	41
Tabel 4.7 Data Serangan Berhasil WPS <i>Cracking</i> .....	44

## DAFTAR GAMBAR

Gambar 4.1 <i>Running Software</i> .....	29
Gambar 4.2 Pemilihan Target.....	30
Gambar 4.3 <i>Handshake Captured</i> .....	31
Gambar 4.4 WPS <i>Cracking Fail</i> .....	31
Gambar 4.5 WPS <i>Cracking Berhasil</i> .....	32
Gambar 4.6 WPA <i>Cracking Berhasil</i> .....	32
Gambar 4.7 WPA <i>Cracking Fail</i> .....	33
Gambar 4.8 WPS PIN <i>Not Found</i> .....	45
Gambar 4.9 <i>Brute Force Denied</i> .....	46
Gambar 4.10 <i>Non-active WPS</i> .....	46
Gambar 4.11 WPS <i>Locked</i> .....	46
Gambar 4.12 DoS <i>Blocked</i> .....	47
Gambar 4.13 Celah Konfigurasi Akses Admin.....	47
Gambar 4.14 <i>Brute Force WPA3</i> .....	48
Gambar 4.15 <i>Brute Force WPA2 Denied</i> .....	48
Gambar 4.16 Bahaya WPS <i>Cracking</i> .....	49



## DAFTAR LAMPIRAN

Lampiran 1 Data Hasil Penelitian

Lampiran 2 Data Serangan WPA *Cracking*

Lampiran 3 Data Serangan WPS *Cracking*



# BAB I

## PENDAHULUAN

### 1.1 Latar Belakang

Penggunaan teknologi *Wireless Fidelity* (Wi-Fi) terus meningkat seiring berjalannya waktu. Hasil survei Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) tahun 2022 menunjukkan angka 20,61% masyarakat Indonesia menggunakan *home* Wi-Fi untuk mendapatkan koneksi internet [1]. Pada tahun 2023, Sekretaris Jenderal APJII Zulfadly Syam mengatakan ada kenaikan pengguna internet rumah (*home* Wi-Fi) sebanyak 0,15% dari tahun sebelumnya serta penurunan pengguna *mobile* data sebanyak 0,33% [2]. Peningkatan ini mulai masif ketika pandemi COVID-19 tahun 2020 yang salah satu penyebabnya adalah pemberlakuan *Work From Home* (WFH) [3]. Hal tersebut yang membuat masyarakat mulai beramai-ramai menggunakan *home* Wi-Fi untuk keperluan akses internet yang dianggap lebih murah dan efisien untuk keperluan sehari-hari. Dikarenakan penggunaannya yang mudah, mulai dari pemasangan sampai perawatan, baik pengguna maupun penyedia layanan cenderung menyepelekan masalah keamanannya dan hanya fokus pada fungsionalnya saja.

Secara umum, kelemahan teknologi *wireless* terbagi menjadi dua yaitu kelemahan konfigurasi dan jenis enkripsi yang digunakan [4]. Pengguna yang awam akan teknologi biasanya hanya memanfaatkan konfigurasi *default* yang telah disediakan oleh penyedia layanan. Penyedia layanan lebih mengutamakan kemudahan akses seperti cara mengganti kata sandi, mengganti nama SSID, atau pihak yang harus dihubungi apabila terjadi masalah daripada perihal keamanan

jaringan. Jenis standar keamanan pada Wi-Fi seperti WEP, WPA, dan WPA2 sudah bukan menjadi fondasi utama dalam mengamankan kata sandi. WPA-PSK yang sekarang banyak digunakan dan salah satu standar keamanan baru juga sudah dapat dipecahkan menggunakan metode *dictionary attack* secara *offline* [5]. Metode keamanan yang tersedia perlu dikombinasikan dengan kesadaran pengguna akan masalah keamanan seperti penggunaan kata sandi yang kuat, penggunaan *firewall*, dan keamanan fisiknya.

Daerah Istimewa Yogyakarta (DIY) menjadi Provinsi dengan indeks literasi digital tertinggi dalam skala nasional pada tahun 2021-2022 [6]. Dalam survei tersebut, skala penentuan sampel di DIY sebesar 74% untuk wilayah perkotaan dari 110 responden. Kota Yogyakarta tentu menyumbang sebagian besar data tersebut dan bisa dikatakan menjadi salah satu kota dengan indeks literasi digital tertinggi. Salah satu bentuk dukungan pemerintah untuk meningkatkan literasi digital masyarakat adalah dengan pengadaan Wi-Fi gratis yang bersifat publik dalam program *Jogja Smart Service* (JSS) dan telah menyediakan setidaknya 524 titik dan akan terus bertambah [7]. JSS juga menjadi bagian penting dalam pengembangan Kota Yogyakarta sebagai *smart city* untuk mewujudkan *smart culture* (*smart education* dan *smart tourism*) [8]. Selain literasi digital, Dinas Pendidikan Pemuda dan Olahraga (Disdikpora) yang bekerja sama dengan Dinas Perpustakaan dan Kearsipan (DPK) berhasil membuat 31 kampung baca hingga akhir 2022 sebagai sentra edukasi masyarakat [9].

Indeks literasi yang tinggi serta program *smart city* menjadi alasan utama peneliti untuk mencari tahu tingkat keamanan *home* Wi-Fi di Kota Yogyakarta terhadap *password attack*. Hal ini dilakukan untuk mengukur seberapa *aware* masyarakat terhadap keamanan *access point* (AP) yang dimiliki sehingga dapat mencegah jenis serangan yang lebih berbahaya.

## 1.2 Rumusan Masalah

Adanya peningkatan pengguna *home* Wi-Fi menandakan ketertarikan masyarakat terhadap teknologi *wireless* khususnya *Wireless Local Area Network* (WLAN). Sedangkan, dalam teknologi *wireless* sendiri terdapat kelemahan yang sering diabaikan penggunaannya yaitu kelemahan konfigurasi dan penggunaan enkripsi. Kota Yogyakarta yang menjadi bagian dari kota dengan indeks literasi digital tertinggi dan program *smart city*-nya belum memiliki data terkait keamanan *home* Wi-Fi yang digunakan oleh sebagian masyarakat. Oleh karena itu, permasalahan yang akan diselesaikan pada penelitian ini adalah Bagaimana tingkat keamanan *home* Wi-Fi di Kota Yogyakarta terhadap *password attack* untuk menghindari akses ilegal dari pihak luar?.

## 1.3 Batasan Masalah

Batasan masalah pada penelitian ini mempertimbangkan kemampuan dari peneliti seperti waktu, biaya, tenaga, dan pengetahuan yang dimiliki. Selain mempertimbangkan sumber daya tersebut, adanya batasan ini juga sebagai gambaran ruang lingkup sejauh mana penelitian ini dilakukan. Oleh karena itu,

peneliti menetapkan batasan-batasan demi kelancaran serta keberhasilan penelitian ini adalah sebagai berikut:

1. Melakukan kajian konsep keamanan jaringan *wireless* berbasis protokol IEEE 802.11 (WLAN).
2. Teknik pengambilan sampel dilakukan menggunakan metode *quota sampling* sebanyak 225 sampel yang diambil dari jaringan *home* Wi-Fi di Kota Yogyakarta.
3. Melakukan uji keamanan jaringan Wi-Fi dengan metode *penetration testing* menggunakan *tools* Wifite pada Kali Linux.
4. Jenis serangan yang digunakan adalah WPA *cracking* dan/atau WPS *cracking*.
5. Kajian keamanan jaringan Wi-Fi dilakukan menggunakan *wireless network adapter* TP-Link TL-WN722N versi 1.10.

#### 1.4 Tujuan Penelitian

Adapun tujuan yang ingin dicapai dari penelitian ini adalah mengetahui persentase tingkat keamanan *home* Wi-Fi di Kota Yogyakarta untuk keperluan data statistik serta bahan edukasi masyarakat terkait keamanan jaringan atau *network security*. Adanya data tersebut diharapkan meningkatkan kesadaran masyarakat terutama di kecamatan/kelurahan yang memiliki persentase keamanan rendah. Data-data tersebut juga digunakan untuk keperluan analisis celah keamanan yang ditemukan sehingga dapat dicari solusi pengamanan yang efektif.

## 1.5 Manfaat Penelitian

Adanya penelitian ini diharapkan memberikan banyak manfaat terutama sebagai bahan edukasi masyarakat terkait seberapa penting masalah keamanan serta risikonya. Data yang terkumpul juga dapat menjadi acuan untuk menilai seberapa aman jaringan *home* Wi-Fi di Kota Yogyakarta sehingga pemerintah setempat dapat menjadikannya acuan dalam membuat program lanjutan terkait teknologi *wireless* atau masalah *security*.





## BAB V

### PENUTUP

#### 5.1 Kesimpulan

Berdasarkan hasil uji *penetration testing* menggunakan metode *password attack* dengan jenis serangan WPA *cracking* dan WPS *cracking* didapatkan kesimpulan sebagai berikut:

- a. Persentase keamanan *home* Wi-Fi di Kota Yogyakarta terhadap *password attack* sebesar 84,44% dari 225 AP yang tersebar di 45 kelurahan. Nilai tersebut terbilang cukup aman dengan latar belakang Kota Yogyakarta sebagai bagian dari Kota dengan indeks literasi tertinggi.
- b. Persentase keamanan tertinggi terletak di Kecamatan Pakualaman dengan persentase 100% dan keamanan terendah Kecamatan Kraton dengan persentase 60%.

#### 5.2 Saran

Saran yang diberikan oleh peneliti terkait keamanan jaringan di Kota Yogyakarta terhadap *password attack* adalah sebagai berikut:

- a. Perlu adanya pemahaman yang cukup untuk mengelola jaringan *home* Wi-Fi terutama masalah keamanannya. Hal ini penting sebagai pengguna untuk mendapatkan fasilitas keamanan yang cukup dari pihak penyedia layanan.

- b. Diharapkan untuk penelitian selanjutnya tidak hanya mengambil data AP saja tetapi juga data pengguna AP dalam bentuk survei/wawancara. Perlu dipertimbangkan juga mekanisme pengambilan sampel seperti tempat dan waktu pengambilan supaya lebih terstruktur dan banyak data yang bisa didapatkan.



## DAFTAR PUSTAKA

- [1] APJII, “Survei Perilaku Penggunaan Internet,” Jakarta, 2022. [Online]. Available: [https://apjii.or.id/download\\_survei/2feb5ef7-3f51-487d-86dc-6b7abec2b171](https://apjii.or.id/download_survei/2feb5ef7-3f51-487d-86dc-6b7abec2b171).
- [2] CNN Indonesia, “Wi-Fi dan Paket Data, Mana yang Lebih Banyak Dipakai Warga Indonesia?,” 2023. <https://www.cnnindonesia.com/teknologi/20230517111117-192-950700/wifi-atau-paket-data-mana-yang-lebih-banyak-dipakai-warga-indonesia> (accessed Feb. 13, 2024).
- [3] Y. Rahmi, “Survei APJII: Pengguna Internet di Indonesia Tembus 215 Juta Orang,” *Bisnis Tekno*, 2023. <https://teknologi.bisnis.com/read/20230308/101/1635219/survei-apjii-pengguna-internet-di-indonesia-tembus-215-juta-orang> (accessed Feb. 13, 2024).
- [4] A. Supriyanto, “Analisis Kelemahan Keamanan pada Jaringan Wireless,” *J. Teknol. Inf. Din.*, vol. 11, no. 1, pp. 38–46, 2006.
- [5] J. M. Sinambela, “Keamanan Wireless LAN ( Wifi ),” in *Seminar Wireless dan Keamanan Wireless*, 2007, no. April, p. 5, [Online]. Available: [https://josh.rootbrain.com/seminar/Makalah Seminar Keamanan Wifi UNY- Josua M Sinambela .pdf](https://josh.rootbrain.com/seminar/Makalah%20Seminar%20Keamanan%20Wifi%20UNY-Josua%20M%20Sinambela.pdf).
- [6] Kemenkominfo, “Status Literasi Digital di Indonesia 2022,” *Kominfo*, no. November, pp. 205–207, 2022, [Online]. Available: <https://www.c2es.org/content/renewable-energy/>.
- [7] Adminwarta, “Penggunaan Teknologi di Kota Yogya Dukung Terciptanya Aktivitas Produktif,” 2021. <https://warta.jogjakota.go.id/detail/index/17442> (accessed Feb. 13, 2024).
- [8] N. Faidat and M. Khozin, “Analisa Strategi Pengembangan Kota Pintar (Smart City): Studi Kasus Kota Yogyakarta,” *JIP (Jurnal Ilmu Pemerintahan) Kaji. Ilmu Pemerintah. dan Polit. Drh.*, vol. 3, no. 2, pp. 171–180, 2018, doi: 10.24905/jip.3.2.2018.171-180.
- [9] Setyono, “31 Kampung Baca di Kota Yogyakarta Berkembang Jadi Sentra Edukasi,” *Eduwara*, 2023. <https://eduwara.com/31-kampung-baca-di-kota-yogyakarta-berkembang-jadi-sentra-edukasi> (accessed Mar. 16, 2024).
- [10] A. T. Sitompul, F. Chahyadi, J. T. Informatika, F. Teknik, U. Maritim, and R. Ali, “Analisis Penerapan Metode Penetration Testing pada Keamanan Jaringan WLAN ( Studi Kasus : Universitas Maritim Raja Ali Haji ),” *J. Sustain. J. Has. Penelit. dan Ind. Terap.*, vol. 12, no. 01, pp. 23–29, 2023.
- [11] N. A. Santoso, M. Ainurohman, S. Y. M. I. Kurniawan, Rifki DwiTegal, and Y. M. I. Tegal, “Penerapan Metode Penetration Testing pada Keamanan

- Jaringan Nirkabel,” *J. Responsif Riset Sains dan Inform.*, vol. 4, no. 2, pp. 162–167, 2022, doi: <https://doi.org/10.51977/jti.v4i2.831>.
- [12] Y. Mulyanto, H. Herfandi, and R. Candra Kirana, “Analisis Keamanan Wireless Local Area Network (WILAN) terhadap Serangan Brute Force dengan Metode Penetration Testing (Studi Kasus:Rs H.L. Manambai Abdulkadir),” *J. Inform. Teknol. dan Sains*, vol. 4, no. 1, pp. 26–35, 2022, doi: 10.51401/jinteks.v4i1.1528.
- [13] R. W. Ismail and R. Pramudita, “Metode Penetration Testing pada Keamanan Jaringan Wireless Wardriving PT . Puma Makmur Aneka Engineering Bekasi,” *J. Mhs. Bina Insa.*, vol. 5, no. 1, pp. 53–62, 2020.
- [14] I. Hossain, M. M. Hasan, S. F. Hasan, and M. R. Karim, “A study of security awareness in Dhaka city using a portable WiFi pentesting device,” in *2019 2nd International Conference on Innovation in Engineering and Technology (ICIET)*, 2019, pp. 1–6, doi: 10.1109/ICIET48527.2019.9290589.
- [15] Y. Ardian, “Buku Ajar Modul 1 Mikrotik Operating System Jaringan Komputer,” *Univ. Kanjuruhan Malang - Fak. Teknol. Inf.*, pp. 1–105, 2016, [Online]. Available: [https://repository.unikama.ac.id/378/1/Modul\\_Jarkom\\_ISBN.pdf](https://repository.unikama.ac.id/378/1/Modul_Jarkom_ISBN.pdf).
- [16] A. Fauzi and A. Maulana, *Jaringan Komputer*. Jakarta: Universitas Nusamandiri, 2018.
- [17] M. K. Qabalin *et al.*, “An Improved Dictionary Cracking Scheme Based on Multiple GPUs for Wi-Fi Network,” *Comput. Mater. Contin.*, vol. 66, no. 3, pp. 2957–2972, 2021, doi: 10.32604/emc.2021.013951.
- [18] S. Rushadi, “Konsep Keamanan Jaringan Komputer dengan Infrastruktur Demilitarized Zone,” *Shar. Knowl. Exp. Konsep*, no. October, pp. 1–5, 2018, [Online]. Available: [https://www.researchgate.net/publication/328130248\\_Konsep\\_Keamanaan\\_Jaringan\\_Komputer\\_dengan\\_Infrastruktur\\_Demilitarized\\_Zone](https://www.researchgate.net/publication/328130248_Konsep_Keamanaan_Jaringan_Komputer_dengan_Infrastruktur_Demilitarized_Zone).
- [19] J. Kaur, “WiFi Security: WEP, WPA, and WPA2,” *Int. J. Control Theory Appl.*, vol. 10, no. May, 2017.
- [20] P. C. van Oorschot, “Wireless LAN Security: 802.11 and Wi-Fi,” in *Computer Security and the Internet*, P. C. van Oorschot, Ed. Cham: Springer International Publishing, 2021, pp. 339–373.
- [21] S. Kwon and H. K. Choi, “Evolution of Wi-Fi Protected Access: Security Challenges,” *IEEE Consum. Electron. Mag.*, vol. 10, no. 1, pp. 74–81, 2021, doi: 10.1109/MCE.2020.3010778.
- [22] Wi-Fi Alliance, “Discover Wi-Fi: Wi-Fi Protected Setup,” 2007. <https://www.wi-fi.org/discover-wi-fi/wi-fi-protected-setup> (accessed Nov. 27, 2023).

- [23] I. D. Rianto, "Anticipating WPS PIN Vulnerability to Secure Wireless Network," *ComTech Comput. Math. Eng. Appl.*, vol. 4, no. 2, pp. 1116–1121, 2013, doi: 10.21512/comtech.v4i2.2554.
- [24] E. Zam, *Buku Sakti Wireless Hacking*. Jakarta: Elex Media Komputindo, 2016.
- [25] A. Ajay, P. P. Amritha, and M. Sethumadhavan, "Automated WPA2 Cracking Using Improved Dictionary and WPS Pin Attack," *Adv. Electr. Comput. Technol. Lect. Notes Electr. Eng.* 711, pp. 323–334, 2021.
- [26] G. Weidman, *PENETRATION TESTING: A Hands-On Introduction to Hacking*. San Francisco: William Pollock, 2014.
- [27] A. Ajay, P. . Amritha, and M. Sethumadhavan, "Automated WPA2 Cracking Using Improved Dictionary and WPS Pin Attack," in *Advances in Electrical and Computer Technologies, Select Proceedings of ICAECT 2020*, Singapore: Springer, 2020, pp. 323–334.
- [28] Sugiyono, *Metode Penelitian Kuantitatif Kualitatif dan R&D*, 19th ed. Bandung: Alfabeta, 2013.
- [29] C. T. Phong and W. Q. Yan, "An Overview of Penetration Testing," *Int. J. Digit. Crime Forensics*, vol. 6, no. 4, pp. 50–74, 2014, doi: 10.4018/ijdcf.2014100104.