E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 02 Nomor 01 Maret 2024

Perancangan *Keylogger* Berbasis *Spyware* untuk Memonitoring Aktivitas Pengguna *Smartphone* Menggunakan Aplikasi *Smart Keylogger*

[1]Sari Wulandari

[12]Pendidikan Teknik Informatika dan Komputer, Universitas Negeri Makassar, Jl. A.P. Pettarani, Kota Makassar, Sulawesi Selatan.

Email: wulandarisari154@gmail.com[1]

Received : 21 Januari 2024
Accepted : 27 Februari 2024
Published : 12 Maret 2024

ABSTRAK

Era teknologi informasi yang semakin berkembang telah menyebabkan meningkatnya ancaman terhadap keamanan dan privasi pengguna komputer dan perangkat mobile, seperti pencurian data dan penggunaan tidak sah. Selain itu, penggunaan internet oleh anak-anak dan remaja juga memerlukan pengawasan khusus. Oleh karena itu penelitian ini memberikan kontribusi pemanfaatan aplikasi *smart keylogger* sebagai solusi yang efektif untuk memantau aktivitas pengguna *smartphone* dan melindungi keamanan data dan privasi pengguna, terutama dalam penggunaan oleh anak-anak dan remaja. Metode penelitian yang digunakan adalah penelitian eksperimental, di mana aplikasi *smart keylogger* diinstal pada *smartphone* pengguna untuk memantau aktivitas pengguna selama periode tertentu. Hasil penelitian menunjukkan bahwa aplikasi *smart keylogger* berjalan dengan baik di latar belakang perangkat, merekam setiap ketukan *keyboard* yang dilakukan pengguna, termasuk riwayat browsing internet dan aktivitas lainnya. Secara keseluruhan, aplikasi *smart keylogger* berbasis *spyware* ini merupakan solusi yang efektif dalam memantau aktivitas pengguna *smartphone*, melindungi keamanan dan privasi data, serta memberikan pengawasan yang lebih efektif dalam penggunaan internet oleh anak-anak dan remaja.

Kata Kunci: *Smart keylogger*, *Spyware*, *Smartphone*, Pengguna, Keamanan

ABSTRACT

The era of growing information technology has led to increasing threats to the security and privacy of computer and mobile device users, such as data theft and unauthorized use. In addition, the use of the internet by children and adolescents also requires special supervision. Therefore this research contributes to the use of the smart keylogger application as an effective solution for monitoring smartphone user activity and protecting user data security and privacy, especially in use by children and adolescents. The research method used is experimental research, in which a smart keylogger application is installed on a user's smartphone to monitor user activity over a certain period. The results of the study show that the smart keylogger application runs well in the background of the device, recording every keystroke the user makes, including internet browsing history and other activities. Overall, this spyware-based smart keylogger application is an effective solution for monitoring smartphone user activity, protecting data security and privacy, and providing more effective monitoring of internet use by children and adolescents.

Keywords: *Smart keylogger, Spyware, Smartphone, User, Security*

E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 02 Nomor 01 Maret 2024

1. PENDAHULUAN

Dalam era teknologi informasi yang semakin berkembang pesat, penggunaan komputer atau perangkat lainnya seperti *smartphone* semakin meluas dan menjadi bagian yang tidak terpisahkan dari kehidupan sehari-hari. Dalam era teknologi informasi yang semakin berkembang pesat, penggunaan komputer atau perangkat lainnya seperti *smartphone* semakin meluas dan menjadi bagian yang tidak terpisahkan dari kehidupan sehari-hari (Hermawan, 2016). Kemudahan akses informasi, komunikasi, dan berbagai layanan online telah mengubah cara kita bekerja, berinteraksi, dan bersosialisasi. Namun, bersamaan dengan manfaat yang ditawarkan, kita juga dihadapkan pada ancaman yang semakin meningkat terkait keamanan dan privasi (Hasibuan, 2016). Salah satu ancaman utama adalah pencurian data, di mana pihak-pihak yang tidak bertanggung jawab dapat mengakses dan mengambil informasi pribadi kita secara ilegal (Javaheri et al., 2018). Data ini dapat digunakan untuk melakukan penipuan, identitas palsu, atau bahkan pencurian identitas. Selain itu, peretasan juga merupakan ancaman serius yang harus dihadapi oleh pengguna komputer dan *smartphone*. Serta penggunaan tidak sah oleh pihak-pihak yang tidak bertanggung jawab juga merupakan masalah yang sering terjadi dalam lingkungan digital Sangat penting bagi pengguna untuk melindungi keamanan data dan privasi mereka (Bonok, 2011).

Pengguna komputer atau *smartphone* serta internet juga tidak terbatas pada orang dewasa, tetapi juga melibatkan anak-anak dan remaja (Masturi et al., 2021). Dalam beberapa tahun terakhir, kemajuan teknologi telah membuat akses internet semakin mudah dan meluas, membawa banyak manfaat dalam hal pendidikan, keterhubungan, dan hiburan (Karlina et al., 2020) . Namun, tidak semua konten yang ada pada internet berkaitan dengan pendidikan atau pengetahuan. Terdapat konten negatif seperti kekerasan, pornografi, penyalahgunaan obat-obatan, perjudian, dan lainnya yang tidak pantas atau tidak boleh diakses oleh anak-anak dan remaja (Aji, 2017). Maka dari itu, orang tua perlu memberikan perhatian khusus dalam memantau aktivitas anak dan remaja dalam menggunakan internet karena semakin beragamnnya informasi pada internet dapat mempengaruhi kehidupan anak dan remaja(Hidayati & Afiatin, 2020). Dengan memantau aktivitas anak, orang tua dapat memastikan bahwa mereka tidak terpapar konten yang tidak pantas atau berbahaya (Hidayat & Maesyaroh, 2022) .

Berdasarkan permasalahan di atas maka diperlukan solusi untuk memantau aktivitas pengguna saat menggunakan komputer atau *smartphone*. Salah satu solusi yang dapat digunakan yaitu dengan menggunakan *keylogger* berbasis *spyware*. *Spyware* adalah sebuah perangkat lunak yang dirancang untuk memata-matai aktivitas pengguna komputer atau perangkat lainnya seperti *smartphone* (Zulfa & Subiyanta, 2015). *Spyware* sering kali dianggap sebagai ancaman keamanan dan privasi yang serius (Tuli & Sahu, 2013). Hal ini karena pengguna tidak menyadari keberadaan dan aktivitas *spyware* pada perangkat mereka, dan data sensitif mereka dapat diakses atau digunakan oleh pihak yang tidak bertanggung jawab(Pandey et al., 2015). Tujuan utama *spyware* adalah untuk mengumpulkan data pribadi atau informasi sensitif pengguna, seperti kata sandi, riwayat penjelajahan web, pesan teks, dan informasi keuangan (Nugraha et al., 2019). *Spyware* dapat merekam ketikan *keyboard* atau dikenal dengan sebutan *keylogger* (Imam et al., 2021). *Keylogger* merupakan salah satu jenis *spyware* yang memiliki kemampuan untuk memata-matai (merekam) ketikan *keyboard* tanpa diketahui oleh pengguna komputer atau perangkat lainnya (Zulfa & Subiyanta, 2015). Biasanya, *keylogger* beroperasi dalam mode latar belakang dan mencatat semua ketukan *keyboard* yang dilakukan oleh pengguna (Navarro et al., 2012).

Dalam jurnal ini, dijelaskan tentang perancangan *keylogger* berbasis *spyware* untuk memonitoring aktivitas pengguna *smartphone* menggunakan aplikasi *smart keylogger*. *Smart keylogger* adalah sebuah aplikasi atau perangkat lunak yang dirancang untuk memantau dan merekam aktivitas pengguna pada perangkat *smartphone* secara diam-diam. Aplikasi ini bekerja dengan merekam semua ketikan yang dilakukan pada *keyboard* perangkat, sehingga memungkinkan pengguna untuk memantau dan mendapatkan informasi tentang aktivitas pengguna, termasuk riwayat penjelajahan web, pesan teks, penggunaan aplikasi, dan lain sebagainya. Oleh karena itu, informasi yang dikumpulkan oleh *smart keylogger* dapat memberikan gambaran lengkap tentang aktivitas pengguna pada *smartphone* dan akses internet. Dengan menggunakan *smart keylogger*, pengguna dapat memantau secara efektif aktivitas pengguna *smartphone*, baik itu anak-anak, remaja, atau bahkan orang dewasa. Para orang tua dapat menggunakan aplikasi ini sebagai alat untuk melindungi anak-anak mereka dari akses ke konten yang tidak sesuai atau berbahaya di internet. Mereka dapat memantau riwayat penjelajahan web anak-anak mereka, pesan teks yang dikirim atau diterima, serta aktivitas penggunaan aplikasi lainnya untuk memastikan keselamatan dan kesejahteraan anak-anak mereka.

E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 02 Nomor 01 Maret 2024

2. STUDI LITERATUR

Beberapa penelitian sebelumnya telah membahas mengenai penggunaan *keylogger* berbasis *spyware* dalam memonitoring aktivitas penggunaan *keyboard* pada sistem komputer. Imam dkk (2021) memfokuskan penelitiannya pada pemanfaatan *keylogger* berbasis *spyware* dalam aspek keamanan untuk memonitoring laptop. Studi ini melibatkan aplikasi Refog Key Logger dalam memantau aktivitas pengguna pada laptop. Penelitian ini menyelidiki efektivitas dan kehandalan *keylogger* dalam melindungi keamanan sistem dan mencegah akses yang tidak sah.

Aji (2017) melakukan penelitian tentang pemanfaatan *keylogger* berbasis *spyware* untuk memonitoring aktivitas penggunaan *keyboard*. Dalam penelitiannya, ia mengidentifikasi risiko keamanan yang terkait dengan penggunaan *keylogger* dan memberikan pemahaman tentang upaya perlindungan yang dapat diambil untuk mengurangi risiko tersebut. Penelitian ini memberikan wawasan tentang cara *keylogger* dapat digunakan sebagai alat pemantauan yang efektif namun juga menyoroti pentingnya mempertimbangkan aspek keamanan dalam penggunaannya.

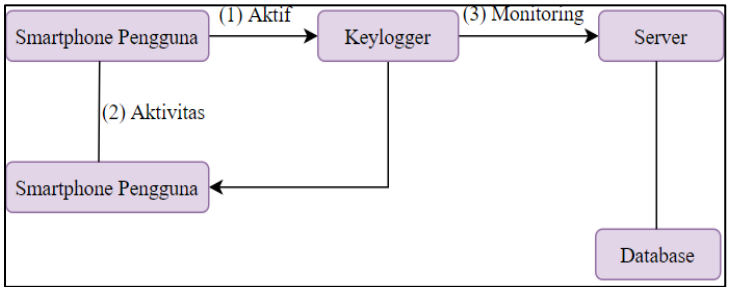
Berdasarkan penelitian-penelitian sebelumnya terkait pemanfaatan *keylogger* berbasi *spyware* dalam memonitoring aktivitas *keyboard* laptop. Terbukti bahwa *keylogger* mampu memantau atau memonitoring aktivitas pengguna. *Keylogger* adalah salah satu jenis *spyware* yang bekerja dengan cara merekam semua ketukan pengguna pada *keyboard*. Melalui studi terkait yang dilakukan sebelumnya, penelitian ini dapat memperluas pemahaman tentang keamanan, privasi, dan pengawasan aktivitas pengguna *smartphone*. Penelitian ini juga memberikan kontribusi pemanfaatan aplikasi *smart keylogger* sebagai solusi yang efektif untuk memantau aktivitas pengguna *smartphone* dan melindungi keamanan data dan privasi pengguna, terutama dalam penggunaan oleh anak-anak dan remaja.

3. METODE PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini adalah Metode Penelitian eksperimental. Metode ini digunakan untuk menguji efektivitas dan efisiensi dari aplikasi aplikasi *Smart keylogger* dalam memonitroing aktivitas pengguna *smartphone*. Penelitian eksperimental dapat dilakukan dengan cara menginstal aplikasi pada komputer atau perangkat target dan memantau aktivitas pengguna selama periode waktu tertentu, sehingga data dapat dikumpulkan dan dianalisis untuk menentukan sejauh mana aplikasi berhasil mengumpulkan informasi yang diinginkan.

Dalam penelitian ini, terdapat beberapa tahap yang penting. Tahap pertama adalah identifikasi masalah, pada tahap ini melakukan identifikasi masalah atau kebutuhan yang ingin diselesaikan melalui perancangan *keylogger* berbasis *spyware* untuk memonitoring aktivitas pengguna *smartphone* menggunakan aplikasi *Smart keylogger*. Tahap Kedua yaitu studi literatur, dilakukan pencarian informasi terkait Aplikasi *Smart keylogger* dan cara kerjanya. Pada tahap ini, dilakukan analisis fungsi dan fitur-fitur *keylogger* serta pemahaman tentang bagaimana *keylogger* dapat digunakan untuk memantau aktivitas pengguna. Tahap Ketiga adalah analisis perangkat lunak, tahap ini dilakukan analisis mendalam terhadap *Smart keylogger* untuk memahami bagaimana program tersebut berfungsi dan berinteraksi dengan sistem operasi dan aplikasi yang sedang berjalan. Tahap terakhir adalah uji coba atau implementasi, dimana sistem yang telah dirancang dan dianalisis diuji untuk memastikan fungsionalitasnya sesuai dengan kebutuhan. Uji coba dilakukan untuk menilai kehandalan dan efektivitas sistem dalam memenuhi kebutuhan yang diinginkan. Hasil dari uji coba ini akan memberikan gambaran tentang kinerja aplikasi *Smart keylogger* dalam memonitoring aktivitas pengguna *smartphone*..

3.1 *Architecture System*



Gambar 1. Arsitektur Sistem

Gambar 1 menjelaskan tentang arsitektur sistem Aplikasi *Smart keylogger*. Pertama, aktivasi *keylogger* dilakukan pada *smartphone* pengguna. Pada tahap ini, aplikasi *Smart keylogger* diaktifkan dan siap untuk merekam aktivitas pengguna. Setelah *keylogger* aktif, semua aktivitas yang dilakukan oleh pengguna pada *smartphone* akan dicatat oleh aplikasi ini. Dalam hal ini, *keylogger* akan merekam setiap ketukan *keyboard* pengguna. Selanjutnya, data yang telah dikumpulkan oleh *keylogger* akan dikirim ke *server* monitoring. *Server* ini berfungsi sebagai tempat penyimpanan sentral untuk semua data yang terkumpul. Dengan demikian, *server* monitoring menjadi pusat pengumpulan dan penyimpanan data pada aplikasi *Smart keylogger*. Pada sisi *server*, terdapat *database* yang digunakan untuk menyimpan semua data dan aktivitas pengguna yang telah dikumpulkan oleh *keylogger*.

Secara keseluruhan, arsitektur sistem *smart keylogger* yaitu aktivasi *keylogger*, pencatatan aktivitas pengguna, pengiriman data ke *server* monitoring, serta penggunaan *database* untuk menyimpan dan mengelola data yang telah dikumpulkan.

3.2 Skema Pengujian

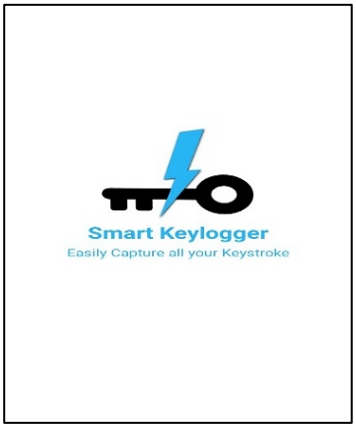
Pengujian aplikasi *Smart keylogger* dalam memonitoring aktivitas pengguna *smartphone* diawali dengan instalasi aplikasi *smart keylogger* pada perangkat pengguna dan melakukan konfigurasi pengaturan aplikasi serta mengaktifkan fungsi *keylogger*. Kemudian melanjutkan dengan melakukan aktivitas menggunakan *keyboard* pada *smartphone*, seperti mengetik dokumen atau melakukan kegiatan lainnya. Selama proses ini, *Smart keylogger* akan merekam semua aktivitas pengguna, termasuk ketikan *keyboard*, pesan yang dikirim, dan aktivitas internet yang dilakukan. Setelah aktivitas pengguna direkam, selanjutnya data yang terkumpul dikirimkan ke *server* untuk disimpan pada *database* aplikasi. Setelah data dikirim ke *server* dan disimpan pada *database*, maka selanjutnya melihat detail aktivitas yang telah dilakukan pada antarmuka aplikasi *Smart keylogger*. Jika pengujian berhasil maka seluruh aktivitas yang dilakukan dengan ketukan *keyboard* akan tampil pada antarmuka aplikasi.

4. HASIL DAN PEMBAHASAN

Aplikasi yang digunakan dalam penelitian ini adalah aplikasi *smart keylogger*. Aplikasi *smart keylogger* diinstall kemudian dijalankan pada *smartphone* pengguna untuk memonitoring aktivitas pengguna.

4.1 Tampilan Aplikasi

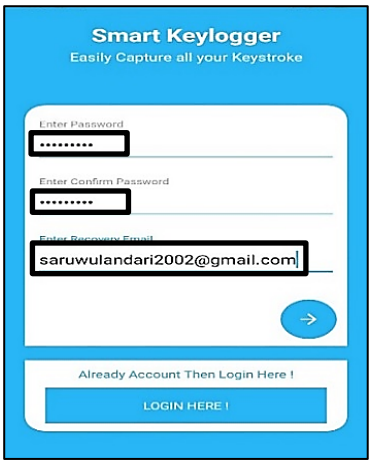
a. Tampilan awal aplikasi *Smart keylogger*



Gambar 2. Tampilan Awal Aplikasi

Gambar 2 merupakan tampilan awal dari aplikasi *smart keylogger* setelah diinstal pada *smartphone* pengguna.

b. Tampilan menu *registrasi* aplikasi *Smart keylogger*.



Gambar 3. Menu Registrasi

Gambar 3 merupakan tampilan pada menu registasi aplikasi *smart keylogger*. Untuk menggunakan aplikasi *Smart keylogger*, pengguna harus terlebih dahulu membuat akun dengan memberikan informasi yang valid dan akurat pada menu registrasi. Seperti memasukkan email dan password serta konfirmasi password.

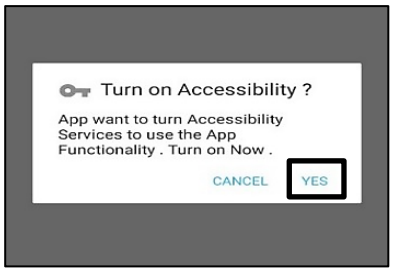
c. Tampilan amsuk pada aplikasi *Smart keylogger*

Gambar 4. Tampilan masuk pada aplikasi

Gambar 4 menjelaskan tentang proses masuk pada halaman utama aplikasi *smart keylogger*. Untuk masuk pada halaman utama aplikasi *smart keylogger* maka pengguna harus memasukkan password yang telah dibuat pada menu registrasi.

4.2 Uji Coba *(Implementasi)* aplikasi

a. Mengatur aksebilitas aplikasi untuk mengakses dan menggunakan aplikasi *smart keylogger*

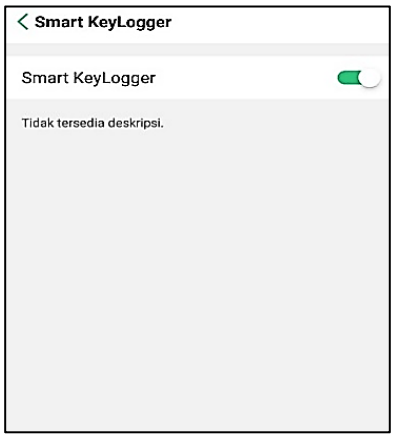


Gambar 5. Mengaktifkan pengaturan aplikasi

Gambar 5 merupakan cara untuk mengatur aksesibilitas aplikasi, artinya mengizinkan atau membatasi izin akses aplikasi terhadap berbagai fitur dan data pada perangkat atau sistem operasi. Ini melibatkan pengaturan kebijakan izin dan preferensi aplikasi *smart keylogger* yang dapat dikendalikan oleh

pengguna. Untuk dapat mengatur dan mengakses aplikasi *smart keylogger* maka pada turn on Accesbility kita klik yes untuk mengaktfikannya.

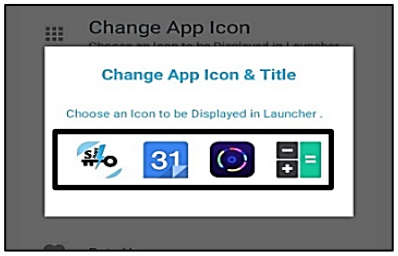
b. Memberikan izin pada aplikasi agar dapat berjalan pada latar belakang aplikasi



Gambar 6. Izinkan Aplikasi

Gambar 6 artinya mengizinkan aplikasi *smart keylogger* untuk tetap aktif dan melakukan tugas meskipun tidak sedang digunakan atau ditampilkan di layar perangkat *smartphone*. Aplikasi *smart keylogger* dapat bekerja dan berjalan pada latar belakang aplikasi agar dapat merekam aktivitas pengguna maka harus diberikan izin terlebih dahulu pada pengaturan *smartphone*.

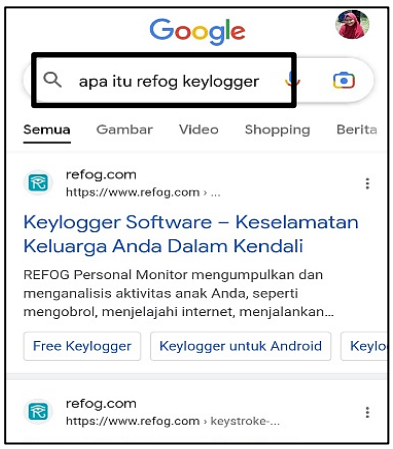
c. Mengubah tampilan *icon* aplikasi *smart keylogger* pada beranda *smartphone*



Gambar 7. Pilihan *icon* aplikasi untuk ditampilkan pada beranda

Gambar 7 menampilkan beberapa pilihan tampilan Icon aplikasi *smart keylogger*. Icon tampilan aplikasi *Smart keylogger* pada beranda dapat diubah menggunakan beberapa pilihan yang disediakan oleh aplikasi agar pengguna tidak mencurigai adanya aplikasi *smart keylogger* pada *smartphone*.

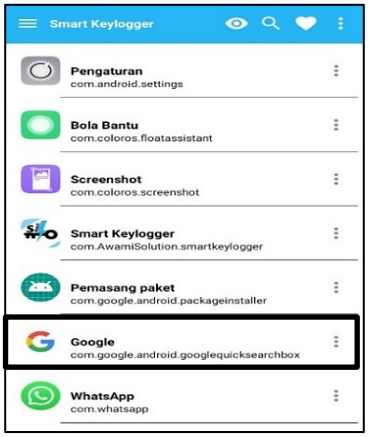
d. Melakukan uji coba dengan melakukan pencarian pada *google* untuk mengetes apakah aplikasi berjalan dengan baik



Gambar 8. Uji coba pada google

Gambar 8 merupakan proses untuk menguji apakah aplikasi *smart keylogger* berjalan dengan baik. Peneliti melakukan pencarian pada google dengan mengetik "apa itu refog *keylogger*". Hal ini dilakukan untuk menguji apakah aplikasi *smart keylogger* mampu merekam ketukan *keyboard* yang dilakukan peneliti pada google.

e. Jika aplikasi berjalan dengan baik dan berhasil maka aktifitas yang dilakukan akan ditampilkan pada antarmuka aplikasi, pengguna dapat melihat detail aktivitas pada *smartphone*



Gambar 9. Tampilan aktivitas pengguna

pada gambar 9 ditampilkan aplikasi-aplikasi yang diakses oleh peneliti pada *smartphone* yang ditampilkan pada antar muka aplikasi *smart keylogger*. Berdasarkan pada gambar 8 terkait melakukan penelusuran pada aplikasi google, maka aplikasi *smart keylogger* berjalan baik terbukti dengan adanya aplikasi google pada antar muka aplikasi *smart keylogger*. Artinya *smart keylogger* mampu merekam aktivitas peneliti yang di tes menggunakan google.

f. Selanjutnya melihat lebih detail aktivitas yang dilakukan pengguna pada google

Gambar 10. Tampilan Detail Aplikasi

4.3 Hasil Pengujian

Berdasarkan uji coba yang telah dilakukan, aplikasi *Smart keylogger* telah terbukti berjalan dengan baik pada *smartphone* pengguna. Dalam pengujian tersebut, aplikasi *smart keylogger* berhasil memantau dan merekam detail aktivitas pengguna yang terkait dengan penggunaan *keyboard*. Keunggulan utama dari aplikasi *Smart keylogger* adalah kemampuannya untuk tetap aktif dan berjalan di latar belakang saat pengguna menggunakan aplikasi lain di perangkat mereka. Dengan fitur ini, *Smart keylogger* dapat secara terus-menerus merekam aktivitas pengetikan pengguna, bahkan ketika mereka sedang menggunakan aplikasi lain. Setiap teks yang diketikkan oleh pengguna pada *keyboard* perangkat akan di-capture dan direkam oleh aplikasi ini. Informasi yang terkumpul kemudian disimpan dan dapat diakses melalui antarmuka yang disediakan oleh aplikasi *Smart keylogger*.

Antarmuka aplikasi *Smart keylogger* memungkinkan pengguna untuk melihat dan menganalisis detail

aktivitas yang telah direkam. Mereka dapat menjelajahi data yang tercatat, melihat teks yang diketikkan pengguna, melacak pesan yang telah dikirim, dan memantau aktivitas internet yang dilakukan

5. KESIMPULAN DAN SARAN

Penelitian yang dilakukan yaitu melakukan eksperimen menggunakan aplikasi *smart keylogger* sebagai solusi untuk memantau aktivitas pengguna *smartphone* dan melindungi keamanan data dan privasi pengguna, terutama anak-anak dan remaja. Berdasarkan penelitian yang telah dilakukan dapat disimpulkan bahwa aplikasi *Smart keylogger* dapat dimanfaatkan untuk memantau atau memonitoring aktivitas pengguna *smartphone* secara rutin. *Keylogger* memungkinkan pengawasan yang efektif terhadap aktivitas pengguna pada perangkat *smartphone*. Pemilik perangkat dapat memantau aktivitas pengguna seperti pengetikan teks, pesan, atau kata sandi yang dimasukkan melalui aplikasi *keylogger*. Penggunaan *Smart keylogger* sebagai program *spyware* tidak memerlukan banyak sumber daya. *Keylogger* dapat beroperasi dengan penggunaan sumber daya yang relatif rendah pada *smartphone*. Hal ini memungkinkan *keylogger* berjalan dengan efisien tanpa memberatkan kinerja perangkat atau terdeteksi dengan mudah oleh pengguna.

Aplikasi ini memberikan kontribusi dalam memantau aktivitas pengguna *smartphone* secara efektif, melindungi keamanan data dan privasi, serta memberikan pengawasan yang lebih efektif dalam penggunaan internet oleh anak-anak dan remaja. Dengan menggunakan aplikasi *smart keylogger*, orang tua dapat memastikan bahwa anak-anak mereka tidak terpapar konten yang tidak pantas atau berbahaya di internet. Mereka dapat memonitor riwayat penjelajahan web anak-anak, pesan teks yang dikirim atau diterima, dan aktivitas penggunaan aplikasi lainnya untuk menjaga keselamatan dan kesejahteraan anak-anak mereka. Dalam penelitian ini, juga diketahui bahwa *spyware* berbasis *smart keylogger* dapat menjadi ancaman terhadap keamanan dan privasi pengguna. Oleh karena itu, perlu mempertimbangkan aspek keamanan dalam penggunaan aplikasi ini.

REFERENSI

Aji, A. B. (2017). Pemanfaatan *Keylogger* Berbasis *Spyware* untuk Memonitoring Aktivitas Penggunaan *Keyboard* User. *Prosiding SNATIF Ke-4 Tahun 2017*, 153–160.

Bonok, Z. (2011). Pentingnya Apliaksi Penanganan *Spyware* untuk Keamanan Privasi User pada Sebuah Komputer. *Saintek*, *6*(1), 1–11. http://www.ainfo.inia.uy/digital/bitstream/item/7130/1/LUZARDO-BUIATRIA-2017.pdf

Hasibuan, M. S. (2016). *Keylogger* pada Aspek Keamanan Komputer. *Teknovasi*, *3*(1), 8–15.

Hermawan, R. (2016). Analisa Cara Kerja dan Dampak dari Serangan Virus *Spyware*. *STRING (Satuan Tulisan Riset Dan Inovasi Teknologi)*, *1*(1), 10–18. https://doi.org/10.30998/string.v1i1.964

Hidayat, A., & Maesyaroh, S. S. (2022). Analisis Penggunaan Gadget pada Anak Usia Dini. *JURNAL SYNTAX IMPERATIF : Jurnal Ilmu Sosial Dan Pendidikan*, *1*(5), 356. https://doi.org/10.36418/syntax-imperatif.v1i5.159

Hidayati, I., & Afiatin, T. (2020). Peran Kontrol Diri dan Mediasi Orang Tua terhadap Perilaku Penggunaan Internet Secara Berlebihan. *Gadjah Mada Journal of Psychology (GamaJoP)*, *6*(1), 43. https://doi.org/10.22146/gamajop.52744

Imam, C., Siregar, M. F., Informasi, T., Battuta, U., Mada, J. G., No, M., Informatika, P., Battuta, U., Mada, J. G., & No, M. (2021). *Pemanfaatan Keylogger dalam Aspek Keamanan Berbasis Spyware untuk Memonitoring Laptop Menggunakan Refog Key Logger*. *10*(1), 105–111.

Javaheri, D., Hosseinzadeh, M., & Rahmani, A. M. (2018). Detection and elimination of *spyware* and ransomware by intercepting kernel-level system routines. *IEEE Access*, *6*, 78321–78332. https://doi.org/10.1109/ACCESS.2018.2884964

Karlina, D. A., Aeni, A. N., & Syahid, A. A. (2020). Mengenal Dampak Positif dan Negatif Internet Untuk Anak pada Orang Tua. *Jurnal Pasca Dharma Pengabdian Masyarakat*, *1*(2), 53–56.

https://ejournal.upi.edu/index.php/JPDPM/article/view/24002

Masturi, H., Hasanawi, A., & Hasanawi, A. (2021). Optimasi Gadget dan Implikasinya Terhadap Pola Asuh Anak. *Jurnal Inovasi Penelitian*, *1*(10), 1–208.

Navarro, J., Naudon, E., & Oliveira, D. (2012). Bridging the semantic gap to mitigate kernel-level *keylogger*s. *Proceedings - IEEE CS Security and Privacy Workshops, SPW 2012*, 97–103. https://doi.org/10.1109/SPW.2012.22

Nugraha, J. D., Budiono, A., & Almaarif, A. (2019). Analisis Malware Berdasarkan API Call Memory Dengan Metode Deteksi Signature-Based. *Jurnal Rekayasa Sistem & Industri (JRSI)*, *6*(02), 77. https://doi.org/10.25124/jrsi.v6i02.351

Pandey, K., Naik, M., Qamar, J., & Patil, M. (2015). *Spyware* Detection Using Data Mining. *International Journal of Engineering and Techniques*, *1*(2), 5–8. http://www.ijetjournal.org

Tuli, P., & Sahu, P. (2013). *Pemantauan Sistem dan Penggunaan Keamanan Keylogger*. 106–111.

Zulfa, M. I., & Subiyanta, E. (2015). Pemanfaatan *Spyware* Untuk Monitoring Aktivitas *Keyboard* Dalam Jaringan Microsoft Windows. *Emitor: Jurnal Teknik Elektro*, *15*(1), 11–14. https://doi.org/10.23917/emitor.v15i1.1752