

## Analisis Peran Pembaruan Sistem Operasi terhadap Keamanan Perangkat *Smartphone*: Studi Literatur

Mohammad Irham Fastabie<sup>1</sup>, Ayub Assabiq<sup>2</sup>, Kamilia Inas Zahira<sup>3</sup>, Risma Aulia Febrianti<sup>4</sup>, Muhammad Daffa Aqila Hakam<sup>5</sup>

Prodi Informatika, Fakultas Sains dan Teknologi, UIN Sultan Maulana Hasanuddin Banten

E-mail: 241730012.mohammadirhamfasatbie@uinbanten.ac.id<sup>1</sup>,

241730011.ayubassabiq@uinbanten.ac.id<sup>2</sup>, 241730033.kamiliainaszahira@uinbanten.ac.id<sup>3</sup>,

241730013.rismaauliafebrianti@uinbanten.ac.id<sup>4</sup>,

241730024.muhammaddaffaaqilahakam@uinbanten.ac.id<sup>5</sup>

### Article History:

Received: 09 Maret 2026

Revised: 18 Maret 2026

Accepted: 29 Maret 2026

**Keywords:** *Pembaruan Sistem Operasi, Keamanan Smartphone, Studi Literatur*

**Abstract:** *Keamanan perangkat smartphone menjadi isu yang semakin penting seiring dengan meningkatnya ketergantungan pengguna terhadap perangkat tersebut dalam menyimpan dan mengelola data sensitif. Sistem operasi sebagai komponen utama perangkat smartphone memiliki peran sentral dalam menjaga keamanan, salah satunya melalui mekanisme pembaruan sistem operasi. Pembaruan sistem operasi tidak hanya bertujuan untuk menambah fitur, tetapi juga untuk menutup celah kerentanan keamanan melalui penerapan patch keamanan secara berkala. Penelitian ini bertujuan untuk menganalisis peran pembaruan sistem operasi terhadap keamanan perangkat smartphone berdasarkan hasil kajian dari berbagai literatur ilmiah. Metode penelitian yang digunakan adalah studi literatur dengan pendekatan kualitatif deskriptif, yaitu menganalisis jurnal dan publikasi ilmiah yang relevan dengan topik pembaruan sistem operasi dan keamanan perangkat smartphone. Hasil analisis menunjukkan bahwa pembaruan sistem operasi berperan penting dalam mengurangi risiko serangan malware, eksploitasi kerentanan, dan kebocoran data pengguna. Namun, efektivitas pembaruan sistem operasi masih menghadapi tantangan, seperti fragmentasi sistem operasi, keterlambatan distribusi pembaruan oleh produsen perangkat, serta rendahnya kesadaran pengguna dalam melakukan pembaruan. Oleh karena itu, diperlukan peran aktif dari pengembang sistem operasi, produsen perangkat, dan pengguna untuk memastikan pembaruan sistem operasi dapat diterapkan secara optimal guna meningkatkan keamanan perangkat smartphone.*

### PENDAHULUAN

Perkembangan teknologi digital yang pesat telah menjadikan *smartphone* sebagai perangkat yang memiliki peran penting dalam kehidupan sehari-hari, baik untuk keperluan pribadi maupun

profesional. *Smartphone* saat ini digunakan untuk menyimpan dan mengelola berbagai data sensitif, seperti informasi perbankan, kredensial akun, serta data lokasi pengguna. Kondisi tersebut menjadikan keamanan perangkat *smartphone* sebagai aspek yang krusial dan memerlukan perhatian serius. Hal ini sejalan dengan kajian yang menyebutkan bahwa meningkatnya fungsi *smartphone* berbanding lurus dengan meningkatnya risiko keamanan data pengguna pada perangkat bergerak Cahyasari Kartika Murni dkk. (2024).

Seiring dengan meningkatnya penggunaan *smartphone*, ancaman keamanan terhadap perangkat bergerak juga terus berkembang. Berbagai kerentanan dan celah keamanan ditemukan pada sistem operasi *smartphone*, baik yang disebabkan oleh kelemahan desain perangkat lunak maupun eksploitasi oleh pihak yang tidak bertanggung jawab. Sistem operasi *smartphone* memiliki peran sentral dalam menjaga keamanan perangkat karena sistem operasi berfungsi sebagai pengelola utama akses aplikasi, data, serta sumber daya perangkat. Navantino dkk. (2025) dalam studi literturnya menyatakan bahwa mekanisme keamanan pada sistem operasi *mobile*, khususnya Android dan iOS, menjadi faktor utama dalam perlindungan data dan privasi pengguna.

Pembaruan sistem operasi merupakan salah satu mekanisme utama yang disediakan oleh pengembang untuk meningkatkan keamanan perangkat *smartphone*. Pembaruan ini tidak hanya berfokus pada penambahan fitur, tetapi juga mencakup penambalan keamanan (*security patch*) yang bertujuan untuk menutup celah kerentanan yang dapat dimanfaatkan oleh *malware* atau peretas. Namun, efektivitas pembaruan sistem operasi sering kali dipengaruhi oleh berbagai faktor, seperti keterlambatan adopsi pembaruan dan fragmentasi sistem operasi, terutama pada ekosistem Android. Cahyasari Kartika Murni dkk. (2024) menegaskan bahwa fragmentasi sistem operasi Android menjadi salah satu tantangan utama dalam penerapan pembaruan keamanan secara merata pada perangkat pengguna.

Berdasarkan kondisi tersebut, diperlukan kajian yang komprehensif untuk memahami peran pembaruan sistem operasi dalam meningkatkan keamanan perangkat *smartphone*. Oleh karena itu, penelitian ini dilakukan menggunakan metode studi literatur untuk menganalisis peran pembaruan sistem operasi terhadap keamanan perangkat *smartphone*, khususnya Android dan iOS berdasarkan hasil penelitian dan publikasi ilmiah sebelumnya. Penelitian ini tidak membahas aspek teknis implementasi secara mendalam, melainkan berfokus pada identifikasi kontribusi pembaruan sistem operasi, jenis ancaman keamanan yang dapat diminimalkan, serta faktor-faktor yang memengaruhi efektivitas pembaruan tersebut. Diharapkan hasil penelitian ini dapat menjadi referensi bagi peneliti, pengembang sistem operasi, dan pengguna dalam memahami pentingnya pembaruan sistem operasi terhadap keamanan perangkat *smartphone*.

## **KAJIAN TEORI**

### **Sistem Operasi pada Perangkat *Smartphone***

Sistem operasi merupakan komponen utama pada perangkat *smartphone* yang berfungsi mengelola perangkat keras, aplikasi, serta interaksi pengguna dengan sistem. Keberadaan sistem operasi memungkinkan perangkat *smartphone* menjalankan berbagai aplikasi sekaligus mengatur akses terhadap sumber daya sistem secara terkontrol. Dalam konteks perangkat bergerak, sistem operasi tidak hanya berperan dalam aspek fungsional, tetapi juga menjadi fondasi utama dalam menjaga keamanan data dan privasi pengguna (Navantino dkk., 2025).

Saat ini, Android dan iOS merupakan dua sistem operasi yang mendominasi pasar *smartphone* global (Counterpoint, 2025). Android dikembangkan dengan pendekatan terbuka dan digunakan oleh berbagai produsen perangkat, sedangkan iOS dikembangkan secara tertutup dan digunakan secara eksklusif pada perangkat Apple (Latif dkk., 2023). Perbedaan arsitektur dan kebijakan pengelolaan sistem operasi tersebut berdampak pada mekanisme pengamanan serta

---

distribusi pembaruan sistem yang diterapkan pada masing-masing platform (Navantino dkk., 2025).

### **Keamanan Perangkat *Smartphone***

Keamanan perangkat *smartphone* menjadi isu penting seiring dengan meningkatnya penggunaan perangkat ini untuk menyimpan dan mengelola data sensitif, seperti informasi pribadi, data keuangan, serta kredensial akun pengguna. Ancaman keamanan pada *smartphone* dapat berasal dari berbagai bentuk, mulai dari *malware*, *spyware*, hingga eksploitasi celah keamanan pada sistem operasi. Oleh karena itu, sistem operasi memiliki peran strategis sebagai lapisan perlindungan utama yang mengatur akses aplikasi dan data pada perangkat.

Beberapa penelitian menunjukkan bahwa kelemahan pada sistem operasi dapat menjadi pintu masuk bagi serangan siber apabila tidak segera ditangani. Cahyasari Kartika Murni dkk. (2024) menyatakan bahwa keamanan pada sistem operasi Android sangat dipengaruhi oleh mekanisme pengelolaan izin aplikasi dan kemampuan sistem dalam menanggapi ancaman keamanan yang terus berkembang. Hal ini menunjukkan bahwa sistem operasi yang tidak diperbarui secara berkala berpotensi meningkatkan risiko keamanan pada perangkat *smartphone*.

### **Pembaruan Sistem Operasi dan Keamanan Perangkat**

Pembaruan sistem operasi merupakan mekanisme penting yang dirancang untuk meningkatkan stabilitas, performa, serta keamanan perangkat *smartphone*. Salah satu komponen utama dalam pembaruan sistem operasi adalah security patch, yaitu pembaruan yang bertujuan untuk menutup celah keamanan yang telah teridentifikasi. Pembaruan keamanan ini berperan dalam mencegah eksploitasi celah oleh *malware* atau pihak yang tidak bertanggung jawab.

Namun, efektivitas pembaruan sistem operasi dalam meningkatkan keamanan perangkat tidak selalu berjalan optimal. Pada ekosistem Android, permasalahan fragmentasi dan keterlambatan distribusi pembaruan menjadi tantangan utama dalam penerapan pembaruan keamanan secara merata (Cahyasari Kartika Murni dkk., 2024). Hal ini sejalan dengan temuan Aura Jelita & Siregar (2025) yang menunjukkan bahwa evolusi ancaman *malware* pada sistem operasi Android menuntut adanya pembaruan keamanan yang konsisten dan tepat waktu.

### **METODE PENELITIAN**

Penelitian ini menggunakan metode studi literatur, yaitu metode penelitian yang dilakukan dengan mengkaji dan menganalisis berbagai sumber pustaka yang relevan untuk memperoleh pemahaman terhadap topik penelitian (Sugiyono, 2013). Pendekatan yang digunakan bersifat kualitatif deskriptif, dengan menganalisis temuan-temuan penelitian terdahulu yang membahas pembaruan sistem operasi dan keamanan perangkat *smartphone*.

Literatur yang dianalisis diperoleh dari jurnal ilmiah yang relevan dengan topik penelitian. Artikel yang digunakan difokuskan pada pembahasan keamanan sistem operasi *smartphone*, mekanisme pembaruan keamanan (*security patch*), serta faktor-faktor yang memengaruhi efektivitas pembaruan sistem operasi. Hasil kajian literatur kemudian dianalisis dan disintesis untuk mengidentifikasi peran pembaruan sistem operasi dalam meningkatkan keamanan perangkat *smartphone*.

### **HASIL DAN PEMBAHASAN**

#### **Ringkasan Literatur**

Berikut ini merupakan ringkasan hasil kajian terhadap sejumlah literatur yang relevan dengan topik penelitian, yaitu peran pembaruan sistem operasi terhadap keamanan perangkat *smartphone*. Literatur yang dianalisis diperoleh dari jurnal ilmiah yang terindeks Google Scholar. Ringkasan literatur disajikan dalam bentuk tabel untuk memudahkan proses perbandingan dan analisis temuan penelitian terdahulu.

No	Penulis & Tahun	Fokus Penelitian	Metode Penelitian	Temuan Terkait Pembaruan OS
----	-----------------	------------------	-------------------	-----------------------------

1.	Navantino dkk. (2025)	Perbandingan sistem keamanan pada Android dan iOS	Studi literatur	Android dan iOS memiliki pendekatan keamanan yang berbeda; iOS lebih tertutup, sedangkan Android lebih fleksibel namun rentan akibat fragmentasi dan keterlambatan pembaruan sistem operasi.
2.	Aura Jelita & Siregar (2025)	Perkembangan ancaman siber dan metode deteksi <i>malware</i> pada Android	<i>Systematic Literature Review</i>	Ancaman <i>malware</i> pada Android terus berkembang seiring waktu; pembaruan sistem operasi dan patch keamanan berperan penting dalam menekan risiko serangan.
3.	Cahyasari Kartika Murni dkk. (2024)	Perkembangan sistem operasi Android dan tantangan keamanannya	Studi Deskriptif	Kompleksitas Android dan keterbukaan sistem meningkatkan risiko keamanan; pembaruan sistem diperlukan untuk menutup celah kerentanan.
4.	Dio Febrillian Tanjung & Wella (2025)	Tingkat keamanan pengguna Android berdasarkan persepsi pengguna	Model <i>Expectancy-Based</i>	Tingkat keamanan perangkat tidak hanya bergantung pada sistem, tetapi juga pada perilaku pengguna dan pemanfaatan fitur keamanan yang tersedia pada OS.
5.	Ahmed & Sallow (2017)	Tinjauan umum keamanan sistem operasi Android.	<i>Literature Review</i>	Android memiliki berbagai kerentanan yang dapat dieksploitasi oleh <i>malware</i> ; sistem keamanan harus diperkuat melalui pembaruan OS secara berkala.
6.	Jones dkk. (2020)	Distribusi dan efektivitas pembaruan keamanan Android	<i>Extensive Quantitative Study</i>	Distribusi patch keamanan Android masih tidak merata karena peran vendor; keterlambatan <i>update</i> meningkatkan risiko keamanan perangkat.
7.	Beyer (2014)	Keamanan perangkat <i>mobile</i> (Android, iOS, BlackBerry)	<i>Literature Review</i>	Ditemukan bahwa Android memiliki banyak kerentanan keamanan, terutama terkait <i>malware</i> , <i>botnet</i> , dan aplikasi palsu. Tingkat pengamanan perangkat <i>mobile</i> masih rendah dan riset solusi masih minim.
8.	Klischies dkk. (2025)	Kerentanan <i>chipset</i> Android	<i>Comprehensive and Empirical</i>	Kerentanan sering diwariskan antar generasi <i>chipset</i> , proses patch lambat, dan banyak

			<i>Study</i>	
				perangkat terdampak tanpa kejelasan <i>update</i> keamanan.
9.	Almanee dkk. (2021)	Sistem operasi Android	LibRARIAN ( <i>LibRARY veRsion IdentificAtioN</i> )	Menunjukkan bahwa kompleksitas sistem Android meningkatkan potensi celah keamanan dan membutuhkan pendekatan keamanan berlapis.
10.	(Khan dkk., 2022)	Keamanan dan privasi <i>mobile</i>	Studi analitis & tinjauan sistem	Menegaskan bahwa lemahnya kontrol keamanan aplikasi dan sistem dapat berdampak langsung pada kebocoran data pengguna.

### Pembahasan

Berdasarkan hasil ringkasan literatur yang telah dianalisis, dapat diketahui bahwa pembaruan sistem operasi memiliki peran yang signifikan dalam menjaga dan meningkatkan keamanan perangkat *smartphone*. Beberapa penelitian menunjukkan bahwa sistem operasi, khususnya Android dan iOS, memiliki pendekatan keamanan yang berbeda. Android bersifat lebih terbuka dan fleksibel, namun kondisi tersebut berdampak pada tingginya tingkat fragmentasi perangkat serta keterlambatan distribusi pembaruan sistem operasi, yang pada akhirnya meningkatkan potensi kerentanan keamanan (Jones dkk., 2020; Navantino dkk., 2025).

Hasil studi literatur juga menunjukkan bahwa ancaman keamanan pada perangkat *smartphone* terus berkembang, terutama dalam bentuk malware yang semakin kompleks. Aura Jelita & Siregar (2025) mengungkapkan bahwa pembaruan sistem operasi dan penerapan patch keamanan secara berkala menjadi salah satu mekanisme utama dalam menekan risiko serangan *malware* pada perangkat Android. Temuan ini sejalan dengan penelitian Ahmed & Sallow (2017) serta Beyer (2014) yang menyatakan bahwa banyaknya kerentanan pada sistem operasi Android dapat dieksploitasi apabila perangkat tidak memperoleh pembaruan keamanan secara rutin.

Selain aspek sistem, efektivitas keamanan perangkat *smartphone* juga dipengaruhi oleh faktor lain, seperti perilaku pengguna dan pengelolaan perangkat keras. Penelitian Dio Febrillian Tanjung & Wella (2025) menegaskan bahwa tingkat keamanan perangkat tidak hanya bergantung pada sistem operasi, tetapi juga pada kesadaran pengguna (*User*) dalam memanfaatkan fitur keamanan yang tersedia. Sementara itu, Klischies dkk. (2025) menunjukkan bahwa kerentanan pada *chipset* Android sering kali diwariskan antar generasi perangkat dan tidak selalu mendapatkan pembaruan keamanan yang memadai, sehingga meningkatkan risiko keamanan jangka panjang.

Secara keseluruhan, hasil analisis literatur menunjukkan bahwa pembaruan sistem operasi berperan penting dalam menutup celah keamanan, mengurangi risiko serangan malware, dan menjaga integritas data pengguna. Namun, efektivitas pembaruan tersebut masih menghadapi berbagai tantangan, seperti fragmentasi ekosistem Android, keterlambatan distribusi *patch* oleh vendor, serta rendahnya kesadaran pengguna dalam melakukan pembaruan sistem. Oleh karena itu, diperlukan upaya berkelanjutan dari pengembang sistem operasi, produsen perangkat, dan pengguna untuk memastikan pembaruan sistem operasi dapat diterapkan secara optimal guna meningkatkan keamanan perangkat *smartphone*.

### KESIMPULAN

Berdasarkan hasil analisis terhadap berbagai literatur yang telah dikaji, dapat disimpulkan bahwa pembaruan sistem operasi memiliki peran yang sangat penting dalam menjaga keamanan perangkat *smartphone*. Pembaruan sistem operasi tidak hanya berfungsi untuk menambahkan fitur baru, tetapi juga berperan dalam menutup celah kerentanan keamanan melalui penerapan *patch*

keamanan yang dirilis secara berkala. Dengan adanya pembaruan tersebut, risiko serangan *malware*, eksploitasi celah keamanan, serta kebocoran data pengguna dapat diminimalkan.

Hasil studi literatur juga menunjukkan bahwa efektivitas pembaruan sistem operasi dalam meningkatkan keamanan perangkat *smartphone* masih menghadapi sejumlah tantangan. Faktor-faktor seperti fragmentasi sistem operasi, keterlambatan distribusi pembaruan oleh produsen perangkat, serta rendahnya kesadaran pengguna dalam melakukan pembaruan sistem menjadi kendala utama dalam penerapan pembaruan keamanan secara optimal. Oleh karena itu, keamanan perangkat *smartphone* tidak hanya bergantung pada sistem operasi, tetapi juga dipengaruhi oleh peran pengembang, produsen perangkat, dan perilaku pengguna.

#### **SARAN**

Berdasarkan kesimpulan yang diperoleh, terdapat beberapa saran yang dapat kami berikan. Bagi pengembang sistem operasi dan produsen perangkat, disarankan untuk meningkatkan konsistensi dan kecepatan dalam distribusi pembaruan sistem operasi dan *patch* keamanan agar seluruh perangkat dapat memperoleh perlindungan yang memadai. Selain itu, diperlukan upaya untuk mengurangi fragmentasi sistem operasi, khususnya pada ekosistem Android, guna meningkatkan efektivitas pembaruan keamanan.

Bagi pengguna perangkat *smartphone*, disarankan untuk lebih meningkatkan kesadaran akan pentingnya melakukan pembaruan sistem operasi secara berkala serta memanfaatkan fitur keamanan yang telah disediakan oleh sistem operasi. Sementara itu, bagi peneliti selanjutnya, penelitian ini dapat dikembangkan dengan menggunakan metode eksperimen atau studi kasus langsung pada perangkat *smartphone* untuk mengukur secara empiris pengaruh pembaruan sistem operasi terhadap tingkat keamanan perangkat

#### **DAFTAR REFERENSI**

- Ahmed, O., & Sallow, A. (2017). Android Security: A Review. *Academic Journal of Nawroz University*, 6(3), 135–140. [https://www.researchgate.net/publication/319365702\\_Android\\_Security\\_A\\_Review](https://www.researchgate.net/publication/319365702_Android_Security_A_Review)
- Almanee, S., Unal, A., Payer, M., & Garcia, J. (2021). Too Quiet in the Library: An Empirical Study of Security Updates in Android Apps' Native Code. <https://doi.org/10.48550/arXiv.1911.09716>
- Aura Jelita, N. B., & Siregar, H. (2025). Systematic Literature Review: Evolusi Ancaman Siber Dan Metode Deteksi Malware Di Sistem Operasi Android (2020–2025). *Jurnal Komputer Teknologi Informasi Sistem Informasi (JUKTISI)*, 4(1), 227–235. <https://doi.org/10.62712/juktisi.v4i1.395>
- Beyer, C. (2014). Mobile Security: A Literature Review. *Dalam International Journal of Computer Applications (Vol. 97, Nomor 8)*. <https://doi.org/10.5120/17025-7315/>
- Cahyasari Kartika Murni, Muhammad Syauqi Husin, & Muhammad Rizal Herdiansyah. (2024). Perkembangan OS Android dan Sistem Keamanan Tantangan dan Solusi. <https://doi.org/10.53567/spirit.v16i1.337>
- Dio Febrillian Tanjung, & Wella. (2025). PENGUKURAN KEAMANAN PENGGUNA ANDROID MENGGUNAKAN EXPECTACY BASED MODEL DAN ALTERNATIVE THREAT BASED MODEL. *Dalam Idealis: Indonesia Journal Information System (Vol. 8, Nomor 1)*. <https://doi.org/10.36080/idealisis.v8i1.3180>
- Counterpoint. (2025, November 24). Global Smartphone Sales Share by Operating System. Diakses pada 8 Januari 2026, dari <https://counterpointresearch.com/en/insights/global-smartphone-os-market-share>
- Jones, K. R., Yen, T. F., Sundaramurthy, S. C., & Bardas, A. G. (2020). Deploying Android Security Updates: An Extensive Study Involving Manufacturers, Carriers, and End Users.

- Proceedings of the ACM Conference on Computer and Communications Security, 551–567. <https://doi.org/10.1145/3372297.3423346>
- Khan, S., Yusuf, A., Nand, P., Haider, M., & Khalid Imam Rahmani, M. (2022). A Review of Android and iOS Operating System Security. <https://doi.org/10.1109/ICETSSIS55481.2022.9888847>
- Klischies, D., Mackensen, P., & Moonsamy, V. (2025, Maret 23). Vulnerability, Where Art Thou? An Investigation of Vulnerability Management in Android Smartphone Chipsets. <https://doi.org/10.14722/ndss.2025.241161>
- Latif, N. S. A., Nawi, M. H. M., Nasir, N. N. M., & Herdiana, R. (2023). Stability Analysis of Competition Model of iOS and Android. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, 30(3), 372–382. <https://doi.org/10.37934/araset.30.3.372382>
- Navantino, F. F., Farhan, M., & Rilvani, E. (2025). Tinjauan Literatur: Perbandingan Sistem Keamanan Pada Aplikasi Android dan iOS. 4(1), 22–28. <https://doi.org/10.55123/storage.v4i1.4778>
- Sugiyono. (2013). *Metode Penelitian Kuantitatif, Kualitatif, dan R&D*.
-