

Madani: Jurnal Ilmiah Multidisiplin
Volume 2, Nomor 6, July 2024, Halaman 813-818
 Licenced by CC BY-SA 4.0
 E-ISSN: [2986-6340](https://doi.org/10.5281/zenodo.13119875)
 DOI: <https://doi.org/10.5281/zenodo.13119875>

Pengembangan Sistem Deteksi dan Pencegahan Deepfakes Pada Windows: Keamanan Distribusi Konten

Muh. Alif ¹, Humaera Hamuddin ², Rakhmadi Rahman³

¹²³Sistem Informasi Institut Teknologi Bacharuddin Jusuf Habibie Parepare, Indonesia
 Email: Muhalf1788@gmail.com,

Abstract

Deepfakes detection and prevention systems are needed nowadays. The publication of content made from AI manipulation is a threat in the digital world. This system is used to minimize the distribution of content that can be used by certain individuals to bring down a person or group. The detection carried out focuses on machine learning as the main system. Blockchain as a system that performs storage and verification based on comparing the original content that has been loaded with content that is considered manipulated. It is transparent and has various advantages that provide security for data and users. With the appropriate dataset in machine learning, detection can be done as needed. Machine learning does not reject many datasets to train the model created to be smarter in detection. Deepfakes pose a significant threat to information dissemination. It is necessary to do good and correct prevention and detection so that disinformation does not occur and also so that there is no hoax information.

Keywords: *Windows, Deepfakes, Machine learning, Blockchain, Detection and prevention systems, Content distribution, Hoax*

Abstrak

Sistem deteksi dan pencegahan deepfakes dibutuhkan dimasa sekarang. Publikasi konten yang terbuat dari manipulasi AI menjadi ancaman dalam dunia digital. Sistem ini digunakan dalam meminimalisir distribusi konten yang dapat dimanfaatkan oleh oknum tertentu untuk menjatuhkan seseorang atau kelompok. Pendeteksian yang dilakukan berfokus dalam machine learning sebagai sistem utama. Blockchain sebagai sistem yang melakukan penyimpanan dan verifikasi berdasarkan dari perbandingan konten asli yang telah dimuat dengan konten yang dianggap manipulasi. Bersifat transparan dan memiliki berbagai keuntungan yang memberikan keamanan untuk data maupun pengguna. Dengan dataset yang sesuai pada machine learning maka pendeteksian dapat dilakukan sesuai dengan kebutuhan. Machine learning tidak menolak banyak dataset untuk melatih model yang dibuat agar lebih pintar dalam melakukan pendeteksian. Deepfakes memberi ancaman yang sangat signifikan dalam penyebaran informasi. Perlu dilakukan pencegahan dan pendeteksian yang baik dan benar agar disinformasi tidak terjadi dan juga agar tidak ada informasi hoax

Kata Kunci: *Windows, Deepfakes, Machine learning, Blockchain, Sistem deteksi dan pencegahan, Distribusi Konten, Hoax*

Article Info

Received date: 30 June 2024

Revised date: 10 July 2024

Accepted date: 18 July 2024

PENDAHULUAN

Sistem operasi windows merupakan sistem operasi yang bersifat open source dan popular digunakan kalangan masyarakat. Teknologi sistem informasi yang menjadi salah satu alat dalam pengelolaan, penyediaan, dan pengumpulan data. Informasi tersebut harus bersifat factual dan dapat dipercaya sehingga dapat dimanfaatkan dengan baik oleh pengguna maupun orang lain. Deepfakes menjadi hal yang paling sering muncul saat ini palagi dengan adanya AI yang membantu dalam melakukan manipulasi konten. Perlunya sebuah sistem yang mampu mendeteksi deepfakes sehingga pengelolaan informasi semakin baik dan bermanfaat. Tidak terjadi disinformasi maupun pemanfaatan konten manipulasi yang bersifat merugikan orang lain. (Shen, H., Xu, Y., & Xu, Z, 2020).

Di era digital yang semakin maju, kemajuan teknologi informasi telah membawa dampak signifikan pada berbagai aspek kehidupan, termasuk di bidang komunikasi dan media. Salah satu inovasi yang menonjol adalah kemunculan teknologi deepfake, yang menggunakan teknik pembelajaran mesin untuk menghasilkan video dan audio yang sangat realistis, tetapi sepenuhnya palsu. Meskipun teknologi ini memiliki potensi positif dalam industri hiburan dan pendidikan, ia juga menimbulkan tantangan serius dalam hal keamanan dan kepercayaan informasi. Deepfake dapat

digunakan untuk memanipulasi konten dengan cara yang merugikan, seperti penyebaran berita palsu, penipuan, dan manipulasi citra publik, yang dapat berdampak negatif pada integritas informasi di platform digital. (Chen, Y., & Liu, J, 2020)

Sebagai salah satu sistem operasi yang paling banyak digunakan di dunia, Windows menjadi target utama untuk pengembangan teknologi deepfake dan penyebaran konten palsu. Windows menyediakan berbagai platform dan aplikasi yang memudahkan penciptaan dan distribusi media digital, tetapi juga menghadapi tantangan dalam menjaga keamanan dan integritas konten yang dibagikan melalui sistemnya. Oleh karena itu, penting untuk mengembangkan sistem deteksi dan pencegahan deepfakes yang efektif agar Windows dapat mempertahankan keamanan dan keandalan distribusi kontennya. (Yaga, D., Mell, P., Roby, N., & Scarfone, K. 2019)

Pengembangan sistem deteksi dan pencegahan deepfakes pada Windows melibatkan integrasi berbagai teknologi dan algoritma untuk mendeteksi keaslian konten secara real-time. Sistem ini harus mampu menganalisis video dan audio yang dikirimkan melalui platform Windows untuk mengidentifikasi tanda-tanda manipulasi yang mungkin tidak terlihat oleh mata telanjang. Implementasi solusi deteksi yang efektif memerlukan kolaborasi antara pengembang perangkat lunak, peneliti keamanan siber, dan pihak berwenang untuk menghadapi berbagai teknik dan metode baru yang digunakan dalam pembuatan deepfake. (Ramachandra, R., Mridha, S., Saha, G. K., & Sural, S. 2020).

Selain itu, pengembangan sistem ini juga harus mempertimbangkan faktor-faktor seperti kecepatan deteksi, akurasi, dan dampak pada performa sistem. Solusi deteksi deepfake harus mampu mengidentifikasi konten palsu tanpa menyebabkan penurunan signifikan dalam kinerja sistem atau pengalaman pengguna. Oleh karena itu, penting untuk menyeimbangkan antara tingkat keamanan dan efisiensi operasional dalam desain sistem deteksi dan pencegahan ini. Dalam konteks yang lebih luas, pengembangan sistem deteksi dan pencegahan deepfakes pada Windows merupakan langkah krusial untuk melindungi keamanan informasi dan mencegah penyebaran konten yang merugikan. Dengan meningkatnya prevalensi deepfake dan potensi dampaknya terhadap kepercayaan publik serta keamanan data, upaya untuk meningkatkan teknologi deteksi dan pencegahan akan sangat berperan dalam menjaga integritas dan keandalan informasi di dunia digital. Pendekatan yang komprehensif dan inovatif dalam menangani tantangan ini akan menentukan seberapa efektif Windows dapat mengatasi ancaman deepfake di masa depan. (Qiu, Z., Yao, T., & Mei, T, 2019)

METODE PENELITIAN

Penelitian ini mengadopsi pendekatan deskriptif untuk memahami dan menjelaskan secara mendetail mengenai sistem deteksi dan pencegahan deepfake yang dikembangkan serta cara kerja sistem tersebut. Pendekatan deskriptif bertujuan untuk memberikan gambaran yang jelas tentang komponen-komponen sistem, metode yang diterapkan, serta proses pengujian yang dilakukan untuk mengevaluasi efektivitas sistem (Reddy, K. M. V. P., Ramachandra, M. S., & Usha, M. N. S. 2021).. Melalui pendekatan ini, penelitian akan menguraikan secara terperinci langkah-langkah dalam pembuatan dan penerapan sistem deteksi deepfake pada platform Windows. Penelitian dimulai dengan penentuan topik, yaitu pengembangan sistem deteksi dan pencegahan deepfake. Penentuan topik ini melibatkan identifikasi masalah utama yang ingin dipecahkan dan tujuan penelitian yang ingin dicapai. Dalam konteks ini, topik yang dipilih adalah pengembangan solusi yang dapat mendeteksi dan mencegah penyebaran konten deepfake pada sistem operasi Windows. Penentuan topik ini juga mencakup penilaian terhadap kebutuhan dan tantangan spesifik yang dihadapi dalam konteks distribusi konten digital pada platform Windows. (Rössler, A., Cozzolino, D., Verdoliva, L., Riess, C., Thies, J., & Nießner, M, 2020)

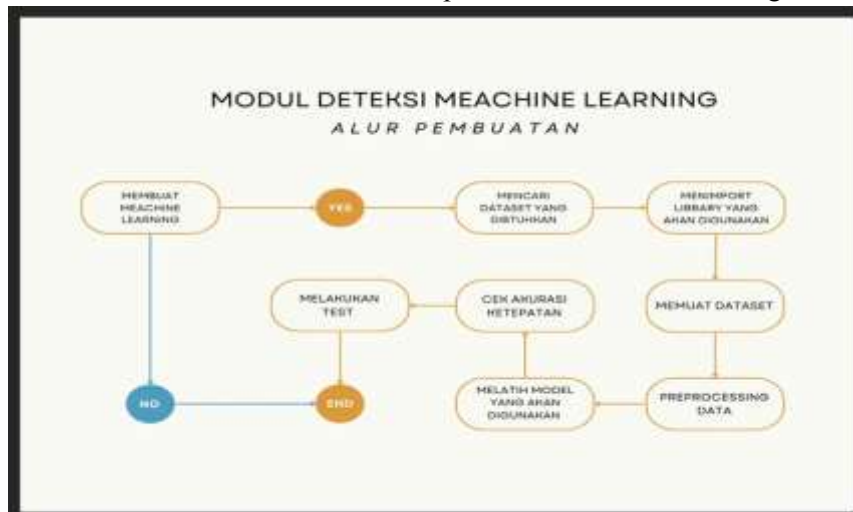
HASIL DAN PEMBAHASAN

1. Modul deteksi deepfake:

Menggunakan model machine learning dalam melakukan pendeteksian. Convolutional Neural Networks (CNN): Digunakan untuk analisis gambar dan video, CNN dapat mendeteksi pola-pola yang tidak terlihat oleh mata manusia yang menunjukkan manipulasi. Recurrent Neural Networks (RNN) dan Long Short-Term Memory (LSTM): Algoritma ini berguna untuk analisis audio dan video berurutan, membantu mendeteksi anomali temporal yang mungkin menunjukkan deepfake. Generative Adversarial Networks (GAN): Selain digunakan untuk membuat deepfakes,

GAN juga bisa dilatih untuk mendeteksi deepfakes dengan memanfaatkan model diskriminatornya yang mampu membedakan antara konten asli dan palsu.

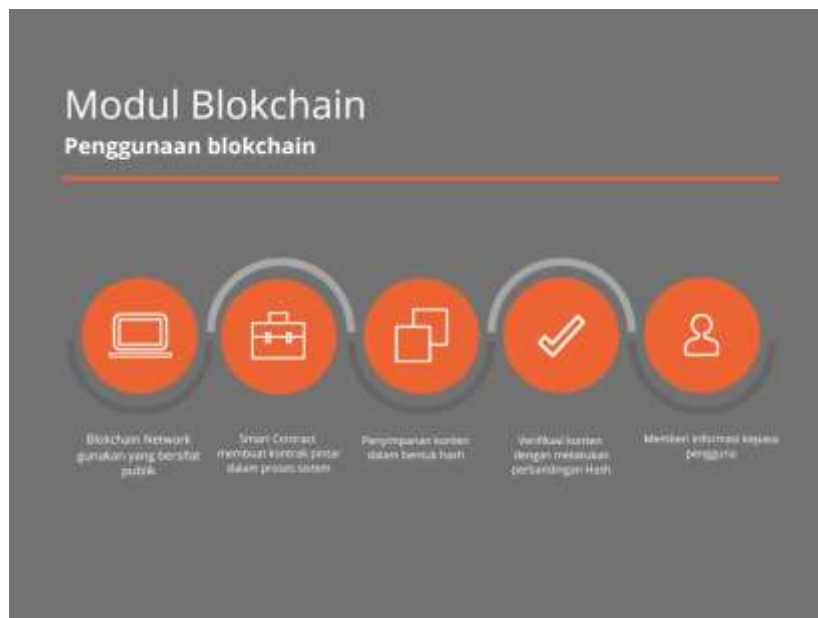
Gambar 1 Desain alur pembuatan machine learning.



2. Modul Blockchain:

Digunakan dalam melakukan verifikasi konten asli dan menjaga integritas data. Verifikasi Sumber: Menyimpan metadata dan hash konten asli di blockchain, sehingga setiap perubahan pada konten dapat diverifikasi terhadap catatan yang tidak dapat diubah di blockchain. Pencatatan dan Pelacakan: Menggunakan blockchain untuk mencatat setiap perubahan atau pemindahan konten, memungkinkan pelacakan asal usul dan perubahan konten. Sertifikasi Keaslian: Menggunakan token non-fungible (NFT) untuk menciptakan sertifikat keaslian konten digital, yang menyertakan informasi tentang penciptaan dan kepemilikan konten.

Gambar 2 Modul Blockchain



3. Modul pengguna:

untuk menampilkan interface antara pengguna dengan sistem. Pada komponen ini berfokus pada desain tampilan antarmuka pengguna. Terkait interface pengguna dapat dilihat melalui link berikut:

<https://www.figma.com/design/37yp1fD6X0YRbIF60X7htf/Untitled?node-id=0-1&t=MHItWAG1R1i4pY0V-1>

4. Api dan Layanan *Backend*: digunakan untuk menghubungkan komponen dari sistem yang dibuat. Segala sistem dari machine learning, blockchain, desain antarmuka dihubungkan menjadi sebuah sistem utuh.
Berdasarkan komponen tersebut dibuat alur kerja dari sistem sebagai berikut:
1. Pengguna atau user mengunggah video maupun gambar yang dimaksud akan dilakukan pengujian ke dalam sistem.
2. Melakukan preprocessing. Sistem akan melakukan preprocessing untuk mengambil fitur penting dalam konten tersebut.
3. Deteksi deepfake yang juga berdasarkan pada model Machine learning yang telah dibuat.
4. Verifikasi Hash yang akan dilakukan oleh blockchain berdasarkan pada dataset pada saat membuat model deteksi. Jika konten asli maka hash akan disimpan dalam blockchain. Jika terdeteksi deepfake maka akan diberikan peringatan pada pengguna.
5. Menampilkan hasil verifikasi kepada pengguna

Sistem yang dibuat diharapkan mampu melakukan deteksi yang akurat terkait manipulasi konten. Dalam hal itu penggunaan dan pemuatan dataset sebagai sumberdaya utama dalam sistem sangat penting dan sangat diperlukan. Untuk sebuah machine learning accuracy menjadi model menjadi tolak ukur dalam pendeteksian. (Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P.(2019)

Gambar 3. contoh hasil pelatihan model machine learning

```
Naive Bayes Train Accuracy: 0.947678117048346
Naive Bayes Train Balanced Accuracy: 0.9476781170483461
Naive Bayes Train Classification Report:

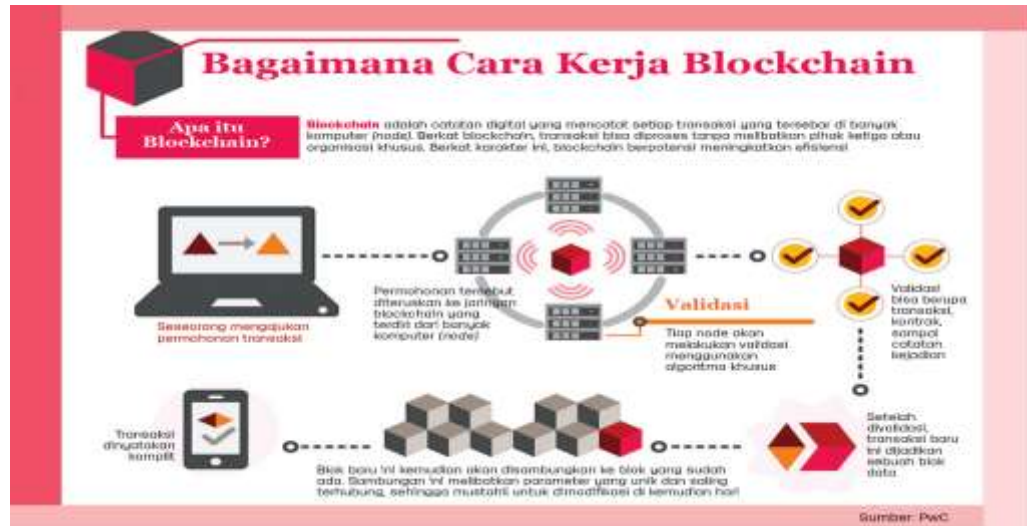
```

	precision	recall	f1-score	support
Demografi	0.97	1.00	0.98	2358
Ekonomi	0.88	0.98	0.93	2358
Geografi	0.99	1.00	1.00	2358
Ideologi	0.96	0.94	0.95	2358
Pertahanan dan kesenian	0.96	0.96	0.96	2358
Politik	0.92	0.77	0.84	2358
Sosial Budaya	0.94	0.95	0.94	2358
Sumber Daya Alam	0.96	0.98	0.97	2358
accuracy			0.95	18864
macro avg	0.95	0.95	0.95	18864
weighted avg	0.95	0.95	0.95	18864

```
Naive Bayes Train Confusion Matrix:
[[2358  0  0  1  0  0  0  0  1]
 [  0 2319  1  0  2 12  7 17]
 [  0  0 2358  0  0  0  0  0]
 [ 18 43  0 2288  5 55  6 23]
 [  6  9  0  7 2162 44 17 13]
 [ 28 199  9  78  69 1828 123 48]
 [ 17 29  1 13  8 27 2247  6]
 [  1 48  1  0  0  1  0 2387]]
```

Accuracy yang tinggi menjadi acuan dalam melakukan validasi terkait dengan dataset baru atau dalam hal konten yaitu konten baru. Setiap hasil akan disimpan dan dapat digunakan kembali sebagai sebuah dataset. Berguna dalam melakukan deteksi yang lebih baik kedepannya. Penggunaan AI bisa menjadi salah satu teknologi yang bisa diimplementasikan kedalam sistem ini. Selain daripada itu blockchain sebagai teknologi yang mengatur dalam penyimpanan dan pengelolaan konten dengan mengubah konten dalam bentuk hash dan dilakukan perbandingan hash untuk mendeteksi konten tersebut. Accuracy yang tinggi menjadi acuan dalam melakukan validasi terkait dengan dataset baru atau dalam hal konten yaitu konten baru. Setiap hasil akan disimpan dan dapat digunakan kembali sebagai sebuah dataset. Berguna dalam melakukan deteksi yang lebih baik kedepannya. Li, D., Xu, Q., & Wang, C. (2021) menyatakan penggunaan AI bisa menjadi salah satu teknologi yang bisa diimplementasikan kedalam sistem ini. Selain daripada itu blockchain sebagai teknologi yang mengatur dalam penyimpanan dan pengelolaan konten dengan mengubah konten dalam bentuk hash dan dilakukan perbandingan hash untuk mendeteksi konten tersebut.

Gambar 4. cara kerja blockchain



Teknologi machine learning sebagai pendeteksi dan juga dapat melakukan verifikasi. Teknologi blockchain pun dapat digunakan dengan menggunakan hash sebagai data yang disimpan dan dibandingkan. Hasil dari sistem yaitu memberikan notifikasi serta menampilkan konten deepfakes dan detail perbedaan dibandingkan konten asli.

SIMPULAN

Pengembangan sistem operasi Windows yang menggabungkan sistem deteksi dan pencegahan deepfakes adalah langkah krusial untuk memperkuat keamanan dalam distribusi konten. Deepfakes, yang memanfaatkan teknologi AI untuk memanipulasi audio dan video, menimbulkan ancaman serius karena kemampuannya menyebarkan informasi palsu dan menipu pengguna. Dengan machine learning dan blockchain sebagai dua komponen utama sehingga pendeteksian dan penverifikasian deepfakes dapat dilakukan. Integrasi teknologi deteksi deepfakes dalam sistem operasi Windows memberikan beberapa keuntungan, seperti peningkatan keamanan konten, perlindungan privasi, peningkatan kepercayaan pengguna, pemanfaatan teknologi AI dan pembelajaran mesin, serta kolaborasi dengan industri. Secara keseluruhan, penerapan sistem deteksi dan pencegahan deepfakes dalam pengembangan sistem operasi Windows adalah langkah strategis untuk mengatasi tantangan keamanan konten digital saat ini.

REFERENCE

- Chen, Y., & Liu, J. (2020). *Deepfake Detection: Current Challenges and Next Steps*. Proceedings of the 2020 ACM Workshop on Information Hiding and Multimedia Security, 71-76.
- Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2019). Blockchain Meets Deep Learning: Security and Privacy Challenges. *IEEE Access*.
- Learning Techniques. *Journal of Information Security and Applications*, 54, 102524.
- Li, D., Xu, Q., & Wang, C. (2021). DeepFake Detection: A Survey. *IEEE Transactions on Information Forensics and Security*. doi:10.1109/TIFS.2021.3056956
- Qiu, Z., Yao, T., & Mei, T. (2019). Combating Deepfakes: A Survey on Detection Techniques and Challenges. *arXiv preprint arXiv:1912.00678*.
- Ramachandra, R., Mridha, S., Saha, G. K., & Sural, S. (2020). TrustNet: A Decentralized Architecture for Detecting Fake Faces in Videos using Blockchain. In *Proceedings of the 2020 IEEE International Conference on Blockchain (Blockchain)*.
- Reddy, K. M. V. P., Ramachandra, M. S., & Usha, M. N. S. (2021). Blockchain-Based Approach for Securing Video Content against Deepfake Attacks. *IEEE Access*, 9, 130826-130838. doi:10.1109/ACCESS.2021.3114073.
- Rössler, A., Cozzolino, D., Verdoliva, L., Riess, C., Thies, J., & Nießner, M. (2020). DeepFakes and Beyond: A Survey of Face Manipulation and Fake Detection. *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*.
- Shen, H., Xu, Y., & Xu, Z. (2020). *Deep Learning for Fake News Detection Using Machine*

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). *Blockchain Technology Overview*. National Institute of Standards and Technology, U.S. Department of Commerce.