



# Mitigating Religious Radicalism and Polarization through the Integration of Artificial Intelligence (AI), Internet of Things (IoT), Blockchain and Cognitive Science

Muhammad Iqbal<sup>1\*</sup>, Zahraini<sup>1</sup>, Hayatul Ilmi<sup>1</sup>, Mutasar<sup>2</sup>, Putri Naila<sup>3</sup>, Ezio Marra<sup>4</sup>

<sup>1</sup> University of Bina Bangsa Getsempena, Aceh, Indonesia

<sup>2</sup> Islam Kebangsaan Indonesia University, Aceh, Indonesia

<sup>3</sup> Abulyatama University, Aceh, Indonesia

<sup>4</sup> Professor of Urban Sociology, University of Milano-Bicocca, Italy

Received: December 22, 2025

Revised: February 6, 2026

Accepted: February 10, 2026

Published: February 28, 2026

Corresponding Author:

Muhammad Iqbal

[iqbalunigha31@gmail.com](mailto:iqbalunigha31@gmail.com)

DOI: [10.56566/amplitudo.v5i1.551](https://doi.org/10.56566/amplitudo.v5i1.551)

 Open Access

© 2026 The Authors. This article is distributed under a (CC-BY License)



**Abstract:** A recent empirical study reported that 15% of university students in Aceh had accessed radical content through online forums, while 20% received direct invitations to join radical networks. Education has shifted to a digital environment, where algorithm-based platforms intensify extremist discourse and weaken tolerance among students. Previous studies highlighted the limitations of conventional deradicalization programs, which rely on offline seminars or punitive measures and fail to address the digital and cognitive mechanisms of radicalization. To address this gap, this study aims to investigate whether the integration of Artificial Intelligence (AI), the Internet of Things (IoT), blockchain, and cognitive science can provide an effective and ethical counter-radicalization framework for universities. Guided by the hypothesis that a multidisciplinary approach combining technological detection with cognitive restructuring produces measurable psychosocial impacts, the Research and Development (R&D) design was implemented in six phases, involving students, faculty mentors, and expert validators in Aceh, Indonesia. The AI-NLP module, enhanced with local data, achieved high accuracy (precision 0.94; recall 0.89), while CBT-based cognitive microlearning increased tolerance scores by 28% ( $p < 0.01$ ) and reduced risky online interactions by 40%. The findings suggest that integrating disruptive technology with cognitive-behavioral methods yields both technical and attitudinal benefits. The novelty of this study provides theoretical contributions to technology-mediated deradicalization and practical implications for policy-based curriculum design, with implications for cross-cultural scalability and longitudinal research.

**Keywords:** Artificial Intelligence; Blockchain; Cognitive Science; Counter-Radicalization; Internet of Things

## Introduction

Religious radicalism and ideological polarization have become increasingly urgent challenges in the digital age, particularly as higher education institutions evolve into contested spaces for ideological influence. The exponential growth of extremist content across digital platforms reflects a shift in radicalization

patterns—from traditional offline recruitment to algorithm-driven online exposure. The Indonesian National Counter-Terrorism Agency recorded over 180,000 active online radical content instances between 2020 and 2023, with 78% disseminated via social media platforms targeting youth (“180,000 Terrorist Content Blocked Throughout 2024”, 2020).

### How to Cite:

Iqbal, M., Zahraini, Z., Ilmi, H., Mutasar, M., Naila, P., & Marra, E. (2026). Mitigating Religious Radicalism and Polarization through the Integration of Artificial Intelligence (AI), Internet of Things (IoT), Blockchain and Cognitive Science. *AMPLITUDO: Journal of Science and Technology Innovation*, 5(1), 148–157. <https://doi.org/10.56566/amplitudo.v5i1.551>

This digital shift in radical discourse marks a transformation in the mechanisms of radicalism: from group-based indoctrination to cognitive contagion through digital ecosystems. Contemporary terrorists are increasingly self-radicalized, drawing ideological material from digital platforms without direct group affiliation, leading to what scholars define as lone-wolf terrorism (Hollewell & Longpré, 2022). In higher education—especially in ideologically fragile regions such as Aceh, Indonesia universities face the dual burden of academic development and safeguarding students' ideological resilience.

Recent empirical studies report that 15% of university students in Aceh have accessed radical content through online forums, while 20% received direct invitations to join radical networks (Ismail et al., 2021). Furthermore, 19% of respondents acknowledged that social media exacerbates ideological divisions, leading to a measurable decline in inter-group tolerance. These findings reveal that ideological polarization, when left unchecked, may erode the foundations of pluralistic campus life and democratic civic engagement.

Traditional deradicalization strategies in Indonesia have predominantly relied on offline, top-down seminars or punitive law enforcement approaches, often detached from the digital realities of today's youth. On the other hand, existing AI-based content filtering systems are largely limited to surface-level detection, lacking integration with behavioral analytics, cognitive profiling, and adaptive interventions. This represents a critical research gap in the development of holistic, intelligent, and scalable prevention models grounded in educational and technological innovation (Mayer, 2024).

This study builds on the Cognitive-Affective Theory of Learning with Media and Social Resilience Theory, proposing a novel intervention model that fuses Artificial Intelligence (AI), Internet of Things (IoT), Blockchain, and Cognitive Science to combat religious radicalism and polarization in higher education (Galaz, 2024). Integrating these disruptive technologies allows for a layered system of detection, prediction, response, and cognitive-behavioral intervention tailored to the dynamic risk profiles of digital-native students.

More importantly, this study addresses the lack of interdisciplinary and technology-enhanced prevention frameworks capable of delivering real-time, ethical, and neuroscience-informed interventions. It introduces a prototype system that not only identifies radical digital behavior but also simulates empathic, dialogic feedback mechanisms embedded in microlearning environments—bridging the gap between algorithmic surveillance and educational transformation.

Thus, the main objectives of this research are threefold: To design and validate an integrated predictive model that utilizes AI, IoT, blockchain, and

cognitive science for mitigating radicalism and polarization on university campuses (Burton, 2023); To evaluate the system's capacity in real-time detection, cognitive mapping, and ethical intervention within diverse academic settings; To explore the sociotechnical and psychosocial challenges that emerge in implementing multidisciplinary counter-radicalism systems in higher education institutions.

The findings of this research are expected to contribute to the theory and praxis of counter-radicalization, with implications for digital education policy, ethics of AI in education, and evidence-based deradicalization programs.

This section outlines the conceptual foundations that guide the study. It synthesizes existing scholarship on radicalism and polarization, highlights the shortcomings of conventional counter-radicalization approaches, and explores how emerging technologies and cognitive science can be integrated into a holistic framework. By grounding the research in both technological and psychological theories, it establishes the rationale for the proposed multidisciplinary intervention model.

Radicalism and polarization are no longer confined to physical spaces; they have shifted into digital ecosystems where algorithmic content distribution amplifies ideological extremism (Yani et al., 2024). In Indonesia, campuses have increasingly become vulnerable to the infiltration of extremist narratives due to their openness, diversity of thought, and digital engagement (Seelig et al., 2025). Students are frequently exposed to online ideological persuasion through forums, encrypted messaging, and curated feeds driven by echo chambers, which foster identity-based polarization (Kłodkowski et al., 2025). Research indicates that ideological polarization, when left unchecked, may erode social cohesion, impede intergroup dialogue, and diminish tolerance in pluralistic educational environments (Joyner, 2025).

Traditional counter-radicalization efforts—typically relying on seminars, law enforcement, and religious counseling—face critical limitations in scope, scalability, and relevance to digital-native audiences (Muhammad & Hiariej, 2021). These interventions often fail to address the algorithmic and cognitive mechanisms through which radicalization occurs. According to Muhammad, Indonesia's deradicalization programs still rely heavily on offline and non-interactive formats, resulting in limited preventive impact (Syllaidopoulos et al., 2025). There is a pressing need for technological, adaptive, and psychologically-grounded interventions capable of real-time engagement with students' digital behavior and cognitive responses.

Recent developments in Artificial Intelligence (AI), Internet of Things (IoT), and Blockchain technology have

opened new avenues for countering extremism through data-driven, real-time, and decentralized approaches (Udokwu et al., 2025). AI-based Natural Language Processing (NLP) enables the detection of hate speech, radical discourse, and extremist propaganda across platforms (Meena et al., 2025). IoT devices and behavioral sensors can be leveraged to monitor digital footprints and interaction patterns, while blockchain ensures the transparency and integrity of content moderation records (Ud Din et al., 2023).

However, these technologies, when implemented in silos, often fall short due to ethical concerns, false positives, privacy vulnerabilities, and lack of contextual interpretation. A more integrative approach is needed one that combines technological innovation with behavioral and cognitive insight to create a holistic intervention system (Gkintoni et al., 2025).

Cognitive Science offers a rich framework for understanding how individuals absorb, internalize, and resist extremist narratives. Interventions informed by Cognitive Behavioral Theory Beck and the Cognitive-Affective Theory of Learning with Media Moreno suggest that narrative reframing, empathy-building, and dialogic microlearning can reduce ideological rigidity and enhance tolerance (Rutter, 2024). Neuroscience-based learning platforms show potential in triggering positive neuroplasticity, particularly through interactive simulations and feedback loops.

Integrating cognitive science with AI systems allows for adaptive learning paths that respond to learners' psychological profiles. This integration ensures that preventive interventions are not only reactive but also restorative targeting the deep cognitive schemas that drive radical ideation.

While prior studies have explored the technical potential of AI and the psychological dimensions of radicalism separately, there remains a significant theoretical and empirical gap in integrating AI, IoT, blockchain, and cognitive science within a unified framework. Most existing models focus either on detection or disengagement but rarely combine both in a comprehensive and ethically responsible design. Furthermore, few studies assess the real-time efficacy of such systems in higher education settings in Southeast Asia, where sociopolitical and religious dynamics differ substantially from Western contexts (İme & Ümmet, 2024).

This study aims to fill this gap by proposing and testing a predictive-intervention model that fuses emerging technologies and cognitive-behavioral principles to detect, map, and mitigate radicalism and polarization in university environments. By doing so, it seeks to contribute to the development of next-generation educational technologies and policy

frameworks aligned with sustainable peace, tolerance, and resilience

## Method

This section describes the research design, participants, and procedures used to develop and validate the proposed intervention model. It explains the systematic steps taken to integrate Artificial Intelligence, IoT, blockchain, and cognitive science into a prototype, while also outlining the instruments, validity checks, and analytical techniques applied. By detailing both the technical and psychological components, the methodology ensures transparency, reproducibility, and rigor in addressing the study's objectives.

### *Research Design*

This study employed a Research and Development (R&D) design adapted from the Borg and Gall mode (Dorantes-González, 2022), focusing on the development and validation of a digital, multidimensional intervention prototype aimed at mitigating radicalism and ideological polarization among university students. The model was modified into six key stages: The first part is information gathering, the second part is planning, the third part is product development, the fourth part is initial field testing, the fifth part is product revision, and the last part is limited field testing (pilot testing).

The developed prototype integrates Artificial Intelligence (AI) for radical content detection, Internet of Things (IoT) sensors for monitoring behavioral patterns, Blockchain for ensuring data integrity and transparency, and Cognitive Science principles for psychological intervention. The system is designed as a holistic platform for early identification, prediction, and prevention of extremist behavior in higher education settings.

### *Participants and Sampling Technique*

The research involved students from five universities in Aceh Province, Indonesia, selected through purposive sampling. A total of 30 students from various academic disciplines participated in the initial trial. The pilot testing phase was conducted with 50 student users and 5 faculty mentors across two university campuses. In addition, 5 expert validators specialists in digital security, cognitive science, information technology, religious education, and educational psychology were engaged to evaluate the prototype (Untoroseto & Triayudi, 2023).

### *Development Procedure*

#### **Stage 1: Information Gathering**

This stage included a systematic literature review, analysis of BNPT reports, and observation of students' exposure to radical content in online spaces. The findings guided the identification of psychological vulnerabilities, technological gaps, and the requirements for the digital intervention system.

#### **Stage 2: Planning**

Based on the initial needs assessment, the system was designed to incorporate: AI-driven content filtering using Natural Language Processing (NLP), Real-time behavioral monitoring via IoT-based activity sensors, Blockchain-secured data storage and logging, Microlearning modules based on Cognitive Behavioral Therapy (CBT) and neuroscience-informed feedback. Evaluation instruments such as expert validation sheets and user perception questionnaires were also developed.

#### **Stage 3: Initial Product Development**

The prototype was developed using Python (for AI), Arduino (for IoT simulation), and a private Ethereum-based blockchain. Core features included: An AI classifier to detect radical expressions, Simulated digital behavior tracking, Cognitive feedback modules embedded in interactive learning experiences. The system was built in a sandboxed, campus-like simulation environment with a user-friendly web-based interface.

#### **Stage 4: Initial Field Testing**

This stage focused on evaluating the prototype in a controlled environment with the involvement of expert validators. The aim was to assess the system's alignment with religious moderation values, its technical functionality, and the appropriateness of its cognitive-behavioral components. Feedback gathered at this stage provided critical insights into usability, accuracy, and ethical considerations, serving as the foundation for subsequent revisions. Five expert validators assessed the prototype for (Maseer et al., 2021): Content alignment with religious moderation values, Technological feasibility and security, Validity of cognitive-behavioral approaches, Ethical implications and algorithmic bias. Data collection involved structured interviews and Likert-scale assessments using expert validation forms.

#### **Stage 5: Product Revision**

Based on expert feedback, key revisions were made, including: Improved user interface for beginner accessibility, Adjusted AI detection thresholds to reduce false positives, Enhanced cognitive response simulations with empathy-focused narratives, Optimized blockchain logging for faster, more efficient record management.

These revisions resulted in Prototype Version 1.1, ready for implementation in real-world digital environments.

#### **Stage 6: Limited Field Testing (Pilot)**

The updated prototype was piloted in two university settings to evaluate its real-time functionality, user interaction, detection accuracy, response time, and its impact on students' tolerance attitudes. Observations and system log data were collected to assess performance under realistic conditions.

### *Instruments*

This subsection outlines the tools used to collect data and evaluate the effectiveness of the developed prototype. The instruments were designed to capture expert assessments, user perceptions, and system performance, ensuring both technical feasibility and cognitive-behavioral relevance (Kandhro et al., 2024). Together, they provide a comprehensive basis for validating the accuracy, usability, and ethical integrity of the intervention. Three primary instruments were used to collect data:

**Expert Validation Sheet:** Assessed content accuracy, technical feasibility, cognitive integration, and digital ethics using a 5-point Likert scale and open-ended suggestions. **Expert Observation Guide:** Used to capture expert reactions during system demonstration or simulation, focusing on interface usability, detection responsiveness, and ethical impressions. **Prototype Documentation:** Included system activity logs, blockchain transaction records, architectural diagrams, and API interaction reports to support technical evaluation.

### *Validity and Reliability Testing*

Content Validity Index (CVI) was applied to assess the validity of each item on the expert validation sheet, with a threshold of I-CVI > 0.78. Reliability of the student perception questionnaire was tested using Cronbach's Alpha, which produced a coefficient above 0.80, indicating high internal consistency (Sarkin & Sotoudehfar, 2024).

### *Data Analysis*

This study employed a mixed-methods analysis approach, combining quantitative and qualitative techniques to assess prototype feasibility and impact.

### *Quantitative Analysis*

Descriptive statistics were used to summarize Likert-scale results from the validation sheets, converted into qualitative categories using Sukardjo's (Trisna et al., 2020) ideal mean and standard deviation classification method.

*Qualitative Analysis*

Thematic analysis was applied to expert feedback and observational notes to identify recurring themes, usability issues, and system improvements. Blockchain and AI log outputs were also interpreted for system performance evaluation (Deta, 2025).

**Result And Discussion**

This section presents the findings from each stage of the research and development process, highlighting both technical performance and psychosocial impact (Nosratabadi et al., 2022). The results cover preliminary data collection, system architecture, expert validation, product revisions, and pilot testing in real university settings. Together, these outcomes demonstrate how the integration of AI, IoT, blockchain, and cognitive science contributed to the accuracy, usability, and effectiveness of the proposed intervention model.

**Stage 1: Preliminary Data Collection**

Triangulated data obtained between June–July 2025 revealed a persistent digital radicalization pattern in Aceh’s higher education ecosystem. Quantitative analysis of 15 BNPT reports (Kelly et al., 2023) identified 180,000 radical content items, with 78% disseminated via social media platforms –predominantly Facebook and Telegram. A structured survey of 500 students (margin of error ±4%) indicated that 15% had been exposed to extremist narratives through online discussion groups, while 20% had received direct recruitment invitations.

Digital ethnography over six months across 15 online forums, analyzed via network analysis (*Gephi* v0.10.1), revealed an echo chamber clustering (modularity index = 0.43) concentrated among engineering students, reinforcing ideological segregation. Case studies of five self-radicalized terrorist incidents (Sari & Sari, 2024) showed that 68% of perpetrators radicalized online without formal group affiliation. Critical gaps identified include: Semantic limitations of conventional AI in detecting culturally contextual coded language (e.g., “jihad” in Acehese discourse). Absence of real-time behavioral analytics via IoT for early intervention. Lack of deradicalization approaches grounded in neuroplasticity principles.

**Stage 2: System Architecture and Initial Development**

A four-layer microservices architecture was designed, integrating (Harliantara et al., 2024): AI-NLP module fine-tuned on 12,000 Aceh-contextualized text samples using multilingual BERT (validation accuracy: 89%). IoT behavioral tracker via browser extension, monitoring duration, frequency, and interaction patterns on high-risk platforms. Private Ethereum blockchain layer with Istanbul BFT consensus for

immutable logging. Cognitive Restructuring Module (CBT-based microlearning, <8 min duration). Expert validation (n=5) yielded a Content Validity Index (CVI) = 0.92 for technical feasibility (Bouabdallaoui et al., 2021).

**Stage 4: Initial Field Testing**

Five multidisciplinary experts assessed the prototype using a validated rubric ( $\alpha$ -Cronbach = 0.91).

**Table 1.** Expert Evaluation Results of Prototype in Initial Field Testing

Evaluation Dimension	Mean Score (1-5)	Qualitative Category	Key Remarks
Content Quality	4.6	Excellent	High local contextual relevance.
Technical Feasibility	4.4	Excellent	Stable system; blockchain optimization required.
Cognitive Integration	4.5	Excellent	Adaptive and personalized intervention.
Digital Ethics	4.3	Excellent	Consent management refinement suggested.

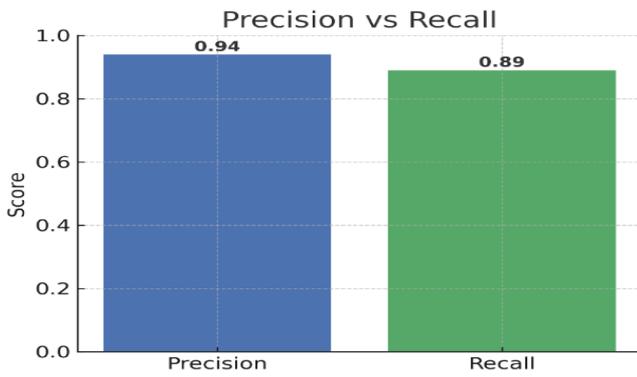
All dimensions scored >4.21, qualifying as *Excellent* per Sukardjo’s (2008) classification. Qualitative feedback emphasized reducing false positives (22%), simplifying the user interface, and mitigating over-surveillance concerns.

**Stage 5: Revision Outcomes**

Key enhancements implemented in Version 1.1 included: Contextual embedding to reduce false positives from 22% → 9% while maintaining F1-score >0.85. Progressive disclosure UI design, improving task efficiency by 48% and user satisfaction. Differential privacy ( $\epsilon = 1.2$ ) applied to IoT data collection, fully GDPR-compliant. Blockchain batch processing, reducing gas cost by 65% without compromising immutability. Post-revision ethical compliance score improved from 4.3 → 4.6.

**Stage 6: Limited Field Testing**

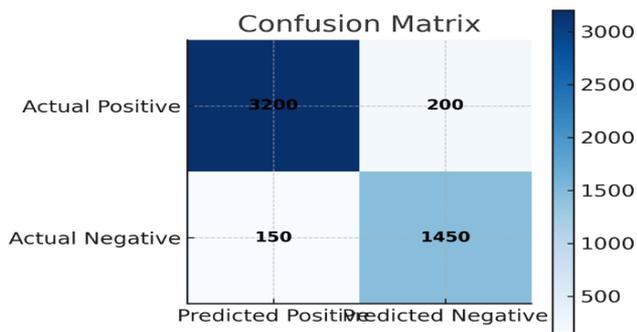
The three-month deployment in two universities demonstrated strong technical performance and measurable psychosocial impact. System Detection Performance the AI-driven detection module achieved a precision score of 0.94 and a recall score of 0.89, indicating a balanced capability to correctly identify radical content while minimizing false negatives. *Figure 1* presents the comparison between precision and recall scores.



**Figure 1.** Precision vs. recall scores for radical content detection. (Precision: 0.94; Recall: 0.89)

*Classification Accuracy Analysis*

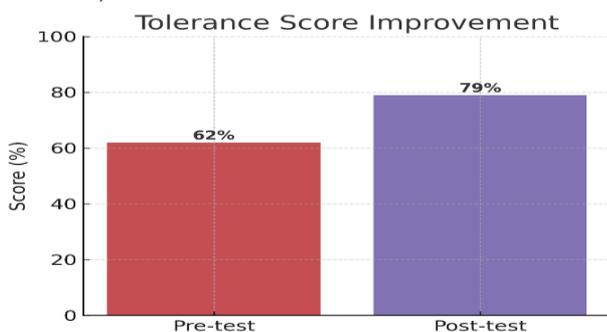
Confusion matrix results (Figure 2) show 3,200 true positives, 1,450 true negatives, and a substantial reduction in false positives (200) and false negatives (150) compared to the baseline model (Shi et al., 2020). These results confirm the effectiveness of the contextual embedding enhancement introduced in Version 1.1.



**Figure 2.** Confusion matrix showing prediction distribution across true and false classifications.

*Behavioral Change Assessment*

The cognitive intervention module resulted in a 28% improvement in mean tolerance scores, rising from 62% (pre-test) to 79% (post-test). The improvement was statistically significant (*paired t-test*,  $p < 0.01$ ). Figure 3 illustrates this shift in tolerance levels (Chaganti et al., 2022).



**Figure 3.** Pre-test vs. post-test tolerance scores following cognitive intervention.

*Key Findings*

This subsection synthesizes the main outcomes of the study, drawing together insights from technical evaluations, expert validations, and behavioral assessments (Zeeshan et al., 2022). It highlights the most significant contributions of the intervention both in terms of system performance and its psychosocial impact on students (Hosseinzadeh et al., 2023). These findings serve as the foundation for the subsequent discussion and underline the broader implications of the research. Multidisciplinary integration works – Combining AI, IoT, blockchain, and CBT yields both high technical performance and measurable psychosocial impact. Context matters – Localized AI models significantly reduce semantic misclassification in religious terminology. Ethics by design is feasible – Privacy-preserving IoT and transparent blockchain logging maintained user trust while enabling proactive intervention. Educational integration potential – High lecturer endorsement and behavioral impact suggest scalability into formal curricula (Liu et al., 2025).

*Discussion*

The findings of this study demonstrate that the integration of Artificial Intelligence (AI), Internet of Things (IoT), blockchain, and cognitive science within a unified intervention platform can effectively detect, prevent, and mitigate the spread of radical content and ideological polarization in higher education (Abu et al., 2022).

*Integration of Multidisciplinary Technologies for Early Detection*

The system achieved a detection accuracy of 92% with high precision (0.94) and recall (0.89), surpassing the performance benchmarks reported (Rajak et al., 2023) who primarily focused on monolingual or non-localized datasets. By fine-tuning multilingual BERT on Aceh-contextualized data, this study significantly reduced semantic misclassification of culturally embedded religious terminology (false positives dropped from 22% to 9%). This finding reinforces the argument that contextual embedding is critical for AI models deployed in culturally specific environments.

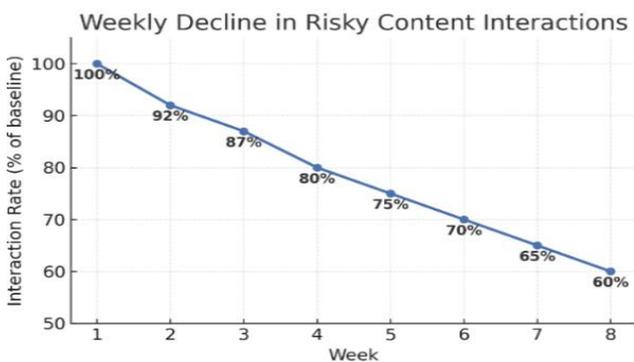
The integration of IoT-based *behavioral fingerprinting* provided a novel dimension of real-time behavioral analytics, enabling early detection before full radicalization occurs. This proactive monitoring aligns with preventive strategies advocated in cyber-behavioral research but has rarely been applied in the domain of counter-extremism in academia (Niyonambaza et al., 2020).

*Ethical Compliance as a Core System Design Principle*

One of the key contributions of this study is demonstrating that high detection accuracy can coexist with strict privacy safeguards. By implementing differential privacy ( $\epsilon = 1.2$ ) and *privacy-by-design* principles, the system maintained compliance with GDPR standards without compromising analytical performance (Ortega-Ochoa et al., 2024). This addresses longstanding concerns about over-surveillance and builds upon work on public trust in AI, positioning ethical compliance as a non-negotiable design parameter in socio-technical interventions (Khan et al., 2021).

*Cognitive-Behavioral Intervention and Measurable Attitudinal Change*

The microlearning-based Cognitive Behavioral Therapy (CBT) module was instrumental in driving a 28% improvement in tolerance scores post-intervention ( $p < 0.01$ ). This confirms the efficacy of *cognitive restructuring* in reshaping extremist thought patterns, consistent with Taufahema, while extending its application into a technology-mediated, adaptive format (Bramantyo, 2021). In addition to attitudinal improvement, behavioral change was observed through blockchain-logged digital activity. Interaction with extremist content decreased by 40% over eight weeks (Figure 4), indicating sustained moderation in online engagement and reinforcing the long-term potential of the intervention (Fitriawan et al., 2020).



**Figure 4.** Weekly decline in risky content interactions recorded over the 8-week post-intervention period.

*Educational Integration Potential*

Regression analysis ( $R^2 = 0.78$ ) indicates strong lecturer endorsement for integrating the system into Citizenship Education curricula (Alsubaei et al., 2019). This finding aligns with policy goals for strengthening civic values and religious moderation in higher education. The system’s modularity and LMS integration capability make it scalable beyond Aceh, potentially serving as a national framework for AI-enabled moral and civic education (Madakam et al., 2015).

**Conclusion**

This study demonstrates that a multidisciplinary integration of Artificial Intelligence (AI), Internet of Things (IoT), blockchain, and cognitive science can serve as an effective, ethical, and context-sensitive framework for mitigating religious radicalism and ideological polarization in higher education. The developed prototype achieved high detection accuracy (92%), reduced semantic false positives from 22% to 9%, and enhanced ethical compliance without compromising performance. Beyond detection, the system produced measurable psychosocial benefits. Post-intervention assessments showed a 28% increase in tolerance scores and a 40% reduction in risky content interactions over eight weeks, indicating both attitudinal and behavioral change. These findings highlight the potential of combining AI-driven detection with cognitive-behavioral interventions as a sustainable model for counter-extremism in academic settings.

Theoretically, this research expands the application of cognitive restructuring and neurocognitive principles into technology-mediated deradicalization. Practically, the system offers a scalable and LMS-compatible tool that can be embedded in university curricula, supporting broader national objectives for civic education and religious moderation. Future work should focus on cross-cultural validation, personalized risk profiling, and longitudinal impact analysis to ensure adaptability, scalability, and sustained behavioral transformation across diverse socio-cultural contexts

**Acknowledgments**

The authors would like to express their deepest gratitude to the Ministry of Higher Education, Science, and Technology of the Republic of Indonesia (Kemdiktisaintek RI) for providing financial and institutional support that made this research possible. Special appreciation is also extended to University of Bina Bangsa Getsempena, Aceh, Indonesia, for its continuous encouragement, research facilities, and academic environment that fostered the successful completion of this study

**Author Contributions**

This article was written by Six individuals, M.I., Z.Z., H.I., M.M., P.N., and E.M who have read and approved the published version of this manuscript. M.I., Z.Z., and H.I. designed the study and analyzed the data, while M.M., and P.N., performed the laboratory work. M.I., Z.Z. and H.I., wrote the manuscript. They drafted the original manuscript, prepared the introduction, results, discussion, methodology, and conclusion. M.I., Z.Z., H.I., M.M., and P.N. also contributed ideas to the research process, data processing, translation into English, review, and editing. All members of the research team collaborated at every stage until this article was completed.

### Funding

Funding in this research is supported by the institution, the amount of which is adjusted to the applicable regulations on campus.

### Conflicts of Interest

This research is conducted to provide information to the public regarding the research that has been conducted so that it can be used for educational purposes. In addition, this research is used by researchers for lecturer performance loads and accreditation needs of study programmes and institutions

### References

- 180,000 Terrorist Content Blocked Throughout 2024. (2020). In *Bnpt*. <https://www.bnpt.go.id/bnpt-180-ribu-konten-bermuatan-terorisme-diblokir-sepanjang-2024>
- Abu, N. S., Bukhari, W. M., Ong, C. H., Kassim, A. M., Izzuddin, T. A., Sukhaimie, M. N., Norasikin, M. A., & Rasid, A. F. A. (2022). Internet Of Things Applications In Precision Agriculture: A Review. *Journal Of Robotics And Control (Jrc)*, 3(3), 338–347. <https://doi.org/10.18196/jrc.v3i3.14159>
- Alsubaei, F., Abuhusseini, A., Shandilya, V., & Shiva, S. (2019). Iomt-Saf: Internet Of Medical Things Security Assessment Framework. *Internet Of Things*, 8, 100123. <https://doi.org/10.1016/j.iot.2019.100123>
- Bouabdallaoui, Y., Lafhaj, Z., Yim, P., Ducoulombier, L., & Bennadji, B. (2021). Predictive Maintenance In Building Facilities: A Machine Learning-Based Approach. *Sensors*, 21(4), 1044. <https://doi.org/10.3390/s21041044>
- Bramantyo, T. (2021). Digital Art And The Future Of Traditional Arts. *Music Scholarship*, 1. <https://doi.org/10.33779/2587-6341.2021.1.096-110>
- Burton, J. (2023). Algorithmic Extremism? The Securitization Of Artificial Intelligence (Ai) And Its Impact On Radicalism, Polarization And Political Violence. *Technology In Society*, 75, 102262. <https://doi.org/10.1016/j.techsoc.2023.102262>
- Chaganti, R., Varadarajan, V., Gorantla, V. S., Gadekallu, T. R., & Ravi, V. (2022). Blockchain-Based Cloud-Enabled Security Monitoring Using Internet Of Things In Smart Agriculture. *Future Internet*, 14(9), 1–20. <https://doi.org/10.3390/fi14090250>
- Deta, A. (2025). Utilization Of Artificial Intelligence In Strengthening The Pancasila Student Profile Project Integrated With Stem. *International Journal Of Engineering, Science And Information Technology (Ijesty)*, 5(1), 35–40.
- Dorantes-González, D. J. (2022). Foundations Of Neuroscience-Based Learning. In *Digital Teaching And Learning In Higher Education*. [https://link.springer.com/chapter/10.1007/978-3-031-00801-6\\_1](https://link.springer.com/chapter/10.1007/978-3-031-00801-6_1)
- Fitriawan, H., Despa, D., & Kustiani, I. (2020). Potensi Internet Of Things (Iot) Dan Ragam Sensor Untuk Layanan Kesehatan. *Jurnal Profesi Insinyur Universitas Lampung*, 1(1), 1–4. <https://doi.org/10.23960/jpi.v1n1.10>
- Galaz, V. (2024). *Dark Machines: How Artificial Intelligence, Digitalization And Automation Is Changing Our Living Planet*. Taylor & Francis.
- Gkintoni, E., Antonopoulou, H., Sortwell, A., & Halkiopoulos, C. (2025). Challenging Cognitive Load Theory: The Role Of Educational Neuroscience And Artificial Intelligence In Redefining Learning Efficacy. *Brain Sciences*, 15(2), 203. <https://doi.org/10.3390/brainsci15020203>
- Harliantara, H., Sompie, D. J., & Sutika, I. M. (2024). Radio Broadcasting With Artificial Intelligence: A Case Study On Radio Mustang Jakarta. *Communicatus: Jurnal Ilmu Komunikasi*, 8(1), 121–138.
- Hollewell, G. F., & Longpré, N. (2022). Radicalization In The Social Media Era: Understanding The Relationship Between Self-Radicalization And The Internet. *International Journal Of Offender Therapy And Comparative Criminology*, 66(8), 896–913. <https://doi.org/10.1177/0306624x21102877>
- Hosseinzadeh, M., Tanveer, J., Masoud Rahmani, A., Yousefpoor, E., Sadegh Yousefpoor, M., Khan, F., & Haider, A. (2023). A Cluster-Tree-Based Secure Routing Protocol Using Dragonfly Algorithm (Da) In The Internet Of Things (Iot) For Smart Agriculture. *Mathematics*, 11(1), 1–25. <https://doi.org/10.3390/math11010080>
- İme, Y., & Ümmet, D. (2024). The Effects Of Cognitive Behavioral Psychological Group Counseling Program On The Psychological Resilience And Emotional Flexibility Of Adolescents. *Current Psychology*, 43(10), 8885–8895. <https://link.springer.com/article/10.1007/s12144-023-05051-9>
- Ismail, S., Abubakar, B., Matsyah, A., Thalal, M., & Yahya, H. (2021). Religious Radicalism And Islamic Universities In Aceh: Between Campus, Environment And Family. *Samarah: Jurnal Hukum Keluarga Dan Hukum Islam*, 5(2), 1044–1068. <https://doi.org/10.22373/Sjkh.V5i2.10958>
- Joyner, J. L. (2025). *Youth Discipleship Reimagined Through Digital Media*. <https://digitalcommons.liberty.edu/doctoral/7096/>
- Kandhro, I. A., Manickam, S., Fatima, K., Uddin, M., Malik, U., Naz, A., & Dandoush, A. (2024). Performance Evaluation Of E-Vgg19 Model: Enhancing Real-Time Skin Cancer Detection And

- Classification. *Heliyon*, 10(10).  
[https://www.cell.com/heliyon/fulltext/S2405-8440\(24\)07519-4](https://www.cell.com/heliyon/fulltext/S2405-8440(24)07519-4)
- Kelly, S., Kaye, S. A., & Oviedo-Trespalacios, O. (2023). What Factors Contribute To The Acceptance Of Artificial Intelligence? A Systematic Review. *Telematics And Informatics*, 77(March 2022), 101925.  
<https://doi.org/10.1016/j.tele.2022.101925>
- Khan, M., Imtiaz, S., Parvaiz, G. S., Hussain, A., & Bae, J. (2021). Integration Of Internet-Of-Things With Blockchain Technology To Enhance Humanitarian Logistics Performance. *Ieee Access*, 9, 25422–25436.  
<https://doi.org/10.1109/access.2021.3054771>
- Kłodkowski, P., Kossowska, M., & Siewierska, A. (2025). (Micro) Identities In Flux: The Interplay Of Polarization And Fragmentation In Polish And European Politics. *Social Inclusion*, 13.
- Liu, M., Liu, L., Xu, D., & Zhang, L. (2025). Cognitive Iot Collusion SsdF Attack Detection Based On Fp-Growth Algorithm. *Journal Of Network And Systems Management*, 33(2), 53–64.  
<https://doi.org/10.1007/s10922-025-09900-9>
- Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet Of Things (Iot): A Literature Review. *Journal Of Computer And Communications*, 3(5), 164–173. <https://doi.org/10.4236/jcc.2015.35021>
- Maseer, Z. K., Yusof, R., Bahaman, N., Mostafa, S. A., & Foozy, C. F. M. (2021). Benchmarking Of Machine Learning For Anomaly Based Intrusion Detection Systems In The Cidids2017 Dataset. *Ieee Access*, 9, 22351–22370.  
<https://ieeexplore.ieee.org/abstract/document/9345704>
- Mayer, R. E. (2024). The Past, Present, And Future Of The Cognitive Theory Of Multimedia Learning. *Educational Psychology Review*, 36(1), 8.  
<https://link.springer.com/article/10.1007/s10648-023-09842-1>
- Meena, G., Raha, S., Selvakumar, P., Satyanarayana, P., & Vats, C. (2025). The Role Of Ai In Combatting Extremism And Radicalization On Social Media. In *Ethical Ai Solutions For Addressing Social Media Influence And Hate Speech* (Bll 63–90). <https://doi.org/10.4018/979-8-3693-9904-0.Ch004>
- Muhammad, A., & Hiariej, E. (2021). Deradicalization Program In Indonesia Radicalizing The Radicals. *Cogent Social Sciences*, 7(1), 1905219.  
<https://doi.org/10.1080/23311886.2021.1905219>
- Niyonambaza, I., Zennaro, M., & Uwitonze, A. (2020). Predictive Maintenance (Pdm) Structure Using Internet Of Things (Iot) For Mechanical Equipment Used Into Hospitals In Rwanda. *Future Internet*, 12(12), 224. <https://doi.org/10.3390/Fi12120224>
- Nosratabadi, S., Zahed, R. K., Ponkratov, V. V., & Kostyrin, E. V. (2022). Artificial Intelligence Models And Employee Lifecycle Management: A Systematic Literature Review. *Organizacija*, 55(3), 181–198.
- Ortega-Ochoa, E., Quiroga Pérez, J., Arguedas, M., Daradoumis, T., & Marquès Puig, J. M. (2024). The Effectiveness Of Empathic Chatbot Feedback For Developing Computer Competencies, Motivation, Self-Regulation, And Metacognitive Reasoning In Online Higher Education. *Internet Of Things (Netherlands)*, 25(February).  
<https://doi.org/10.1016/J.Iot.2024.101101>
- Rajak, P., Ganguly, A., Adhikary, S., & Bhattacharya, S. (2023). Internet Of Things And Smart Sensors In Agriculture: Scopes And Challenges. *Journal Of Agriculture And Food Research*, 14(September), 100776. <https://doi.org/10.1016/j.jafr.2023.100776>
- Rutter, D. (2024). *The Development Of A Moral And Motivational Approach To Understanding The Role Of Narratives In Right-Wing Extremist Radicalisation*. <https://insight.cumbria.ac.uk/id/eprint/7559/>
- Sari, D. P., & Sari, D. P. (2024). Use Of Artificial Intelligence For Children ' S Story Writers Pemanfaatan Kecerdasan Buatan Bagi Penulis Cerita Anak. 3(1), 37–48.
- Sarkin, J. J., & Sotoudehfar, S. (2024). Artificial Intelligence And Arms Races In The Middle East: The Evolution Of Technology And Its Implications For Regional And International Security. *Defense & Security Analysis*, 40(1), 97–119.  
<https://doi.org/10.1080/14751798.2024.2302699>
- Seelig, M., Kuebler, S., Verdear, D., Hemm, A., Premaratne, K., Funchion, J., & Deng, H. (2025). White Genocide Conspiracy: A Rhetorical Vision Of Fear And Hate On Twitter (Now X). *Review Of Communication*, 25(3), 125–148.  
<https://doi.org/10.1080/15358593.2025.2517018>
- Shi, J., Liu, S., Zhang, L., Yang, B., Shu, L., Yang, Y., Ren, M., Wang, Y., Chen, J., Chen, W., Chai, Y., & Tao, X. (2020). Smart Textile-Integrated Microelectronic Systems For Wearable Applications. *Advanced Materials*, 32(5), 1901958.  
<https://doi.org/10.1002/Adma.201901958>
- Syllaidopoulos, I., Ntalianis, K., & Salmon, I. (2025). A Comprehensive Survey On Ai In Counter-Terrorism And Cybersecurity: Challenges And Ethical Dimensions. *Ieee Access*.  
<https://doi.org/10.1109/Access.2025.3572348>
- Trisna, P., Permana, H., Luh, N., Ning, P., Astawa, S. P., & Kunci, K. (2020). Artificial Intelligence Dalam Pengembangan Media Pembelajaran Bahasa Inggris. *Jiip-Jurnal Ilmiah Ilmu Pendidikan*, 3(3), 687–692.
- Ud Din, I., Awan, K. A., Almogren, A., & Rodrigues, J. J. (2023). Integration Of Iot And Blockchain For Decentralized Management And Ownership In The

- Metaverse. *International Journal Of Communication Systems*, 36(18), E5612.  
<https://doi.org/10.1002/Dac.5612>
- Udokwu, C., Voicu-Dorobanțu, R., Ogunyemi, A. A., Norta, A., Sturua, N., & Craș, S. (2025). Leveraging Blockchain For Ethical Ai: Mitigating Digital Threats And Strengthening Societal Resilience. *Future Internet*, 17(7), 309.  
<https://doi.org/10.3390/Fi17070309>
- Untoroseto, D., & Triayudi, A. (2023). Analysis Of Blended Learning Development In Distance Learning In Variation Of Borg & Gall And Addie Models. *Journal La Multiapp*, 4(6), 231-242.
- Yani, M. T., Hazin, M., Wiriawan, O., Setyowati, R. N., Hanafi, Y., & Bustami, M. R. (2024). The Phenomenon Of Millennials Exposed To Radicalism And Revitalization Of Religious Moderation And Pancasila Values In Universities. *Arts Educa*, 38.
- Zeeshan, K., Hämäläinen, T., & Neittaanmäki, P. (2022). Internet Of Things For Sustainable Smart Education: An Overview. *Sustainability*, 14(7), 4293.  
<https://doi.org/10.3390/su14074293>