South American Publishing

SAP Artificial Intelligence in Dentistry. 2026;2:119
doi: 10.62486/aid2026119

REVIEW

Edge computing, Internet of Things and cybersecurity in the deployment of dental artificial intelligence

Computación perimetral, Internet de las cosas y ciberseguridad en el despliegue de la inteligencia artificial odontológica

Diana Anselmo[1]
Stacey Estefan[2]

[1] University of Texas at Austin, Dell Medical School. Austin, Estados Unidos.
[2] University of Washington, School of Medicine, Department of Global Health. Seattle, Estados Unidos.

Submitted: 07-02-2026 | Revised: 11-04-2026 | Accepted: 16-06-2026 | Published: 20-06-2026

Corresponding Author: Stacey Estefan

ABSTRACT

The deployment of dental artificial intelligence depends not only on the accuracy of the models but on the infrastructure that hosts them and the security that protects them, and this narrative review synthesizes the evidence on edge computing, the Internet of Things and cybersecurity as the three determinants of that deployment. The available evidence converges on the conclusion that edge computing reduces latency and preserves privacy but constrains model size, that the Internet of Things extends data collection into the home and the mouth while multiplying the attack surface, and that cybersecurity is the least mature of the three, with adversarial attacks and data governance emerging as the principal risks. The synthesis integrates the dental-specific evidence with the wider edge-computing and medical-device-security literature, and it identifies the hybrid local-cloud architecture and federated learning as the approaches that best reconcile privacy with performance. The review concludes that the technical infrastructure for dental artificial intelligence is maturing faster than the security and governance that its deployment requires, and that the field must close that gap before connected dental intelligence can be deployed at scale.

Keywords: artificial intelligence; edge computing; internet of things; computer security; dentistry.

RESUMEN

El despliegue de la inteligencia artificial odontológica depende no solo de la precisión de los modelos, sino de la infraestructura que los aloja y de la seguridad que los protege, y esta revisión narrativa sintetiza la evidencia sobre la computación perimetral, el Internet de las cosas y la ciberseguridad como los tres determinantes de ese despliegue. La evidencia disponible converge en que la computación perimetral reduce la latencia y preserva la privacidad pero limita el tamaño de los modelos, en que el Internet de las cosas extiende la recogida de datos al hogar y a la boca al tiempo que multiplica la superficie de ataque, y en que la ciberseguridad es la menos madura de las tres, con los ataques adversarios y la gobernanza de datos como principales riesgos. La síntesis integra la evidencia específicamente odontológica con la literatura más amplia sobre computación perimetral y seguridad de dispositivos médicos, e identifica la arquitectura híbrida local-nube y el aprendizaje federado como los enfoques que mejor concilian privacidad y rendimiento. La revisión concluye que la infraestructura técnica de la inteligencia artificial odontológica madura más rápido que la seguridad y la gobernanza que su despliegue requiere, y que el campo debe cerrar esa brecha antes de que la inteligencia dental conectada pueda desplegarse a escala.

Palabras clave: inteligencia artificial; computación perimetral; internet de las cosas; seguridad informática; odontología.

© 2026; The Authors. This Open access article is distributed under CC BY 4.0 licence.

INTRODUCTION

The deployment of dental artificial intelligence is usually discussed as a problem of model accuracy, but the accuracy of a model is only the first of the conditions that determine whether it can be used in practice. A model that classifies a radiograph perfectly is of no practical use if it cannot run where the radiograph is, if the data it needs cannot be collected or moved safely, or if the device that hosts it can be compromised by an attacker. These three conditions, where the model runs, how the data reaches it, and how the whole system is secured against misuse, are the infrastructure of dental artificial intelligence, and they are the subject of this review. The three themes that structure it, edge computing, the Internet of Things and cybersecurity, are therefore not peripheral to the field but the determinants of whether its accurate models ever leave the laboratory and reach the clinic.

The urgency of these questions is rising in step with the pace of the field itself. The dental artificial intelligence models have reached the point of clinical accuracy across detection, diagnosis and planning, and the natural next step is to connect them, to run them at the point of care and to feed them with data from devices beyond the clinic, and it is exactly this next step that the three themes govern. A field that has mastered the model but not the infrastructure will find that its accurate models stall at the very threshold of deployment, and the review is written for the moment at which that threshold is now being crossed. The reader who is deciding how to deploy a dental model, or who is weighing whether to adopt a connected dental device, is the reader for whom these three themes are the practical questions rather than the distant background.

The three themes are tightly coupled, and their coupling is the reason they are reviewed together. Edge computing moves the computation to the device or to the clinic itself to reduce the latency and the privacy exposure of sending data to a cloud, and it is the answer to the question of where a dental model should run. The Internet of Things extends the reach of the system well beyond the clinic, into the patient's home and into the mouth itself, and it is the answer to the question of where the data comes from. Cybersecurity is the constraint that both of the other two impose, because every edge device and every connected sensor is a potential point of compromise for an adversary, and it is the answer to the question of whether the whole system can ultimately be trusted. The three themes therefore describe a single system, the connected and distributed dental intelligence, and the review deliberately treats them as three views of that one system rather than as separate topics.

The intended audience for this review is the practitioner and the developer who must make the deployment decisions, and the review is written for them rather than for the specialist in any one of the three themes. The edge-computing specialist and the cybersecurity specialist will find the treatment of their own theme introductory, and the dental practitioner will find the treatment of the clinical context introductory, and this is deliberate, because the review's contribution is the integration across the three themes rather than the depth within any one. The value of reading the three themes together, rather than separately, is that the trade-offs between them, which are the actual day-to-day decisions of a deployment, become visible only in the combined view, and that combined view is what the review provides.

The objective of this review is to synthesize the evidence on edge computing, the Internet of Things and cybersecurity as the determinants of the deployment of dental artificial intelligence, and to integrate the dental-specific evidence with the wider edge-computing and medical-device-security literature. The review anticipates its axes at the outset: the first axis examines the evidence on edge computing for on-device dental inference, the second the evidence on Internet of Things devices and their role, and the third the evidence on cybersecurity threats and safeguards, with a fourth and final axis on the deployment architectures that combine the other three.

DEVELOPMENT

Edge computing for on-device dental inference

The evidence on edge computing converges on the conclusion that it is the natural host for dental artificial intelligence, and the dental-specific literature echoes the wider edge-intelligence literature in reaching that same judgement. Edge computing moves the inference to the device or to the clinic, which reduces the latency of the classification and, more importantly, keeps the clinical data on site rather than transmitting it to a remote cloud, and these two properties are the reason it is repeatedly proposed as the deployment architecture for dental models.(1-3)The constraint that

edge computing imposes is the size of the model, because an edge device cannot host the largest and most demanding networks, and the lightweight models and the TinyML approaches that the wider literature develops are the direct response to that constraint.(4,5) The dental literature that addresses deployment explicitly reaches the same conclusion, that a local or a hybrid model is the practical answer for a clinic that must keep its patients' radiographs and records on site.(6,7) Eight studies support this axis directly, and they converge on the trade-off between latency and model size as its defining feature.

The privacy motivation behind the edge deployment deserves emphasis, because it is the reason the dental field prefers the edge over the cloud despite the capacity advantage of the latter. A dental radiograph is identifiable clinical data, and the regulatory and ethical requirements that govern its handling are stricter than the requirements that govern, say, an image of a product, so a clinic that sends its radiographs to a cloud is assuming a compliance burden that a local model avoids. The edge therefore answers not merely a technical question but a governance one, and the dental deployment literature is explicit that this, rather than the latency, is the deciding factor for the clinical setting.(6,7) This is why the local and hybrid architectures are proposed even though the cloud could run a larger and more accurate model, and it is the reason the review treats the privacy property as the defining feature of the edge axis rather than as a secondary benefit.

The dental applications that the edge deployment serves are the same applications that dominate the dental artificial intelligence literature, the detection, the diagnosis and the planning, and the edge does not change what the models do but only where they do it. A caries detector that runs on a device in a community screening, a segmentation model that runs in the clinic's own hardware, and a planning model that runs on the workstation are all the same model deployed at the edge rather than in the cloud, and the dental deployment papers describe exactly these cases.(6,8,9)The benefit that the edge confers is therefore not a new capability but a new locus, and the locus matters because it determines the latency, the privacy and the availability of the model. The community screening example is the most instructive, because it is the case in which the edge deployment is not a mere preference but a genuine necessity, there being no reliable connectivity to a cloud in the field setting.(8)This is the axis's practical and settled conclusion: the edge is where the dental model must run whenever the clinic or the field is its intended destination.

The locally executable dental systems provide the concrete demonstration of this axis. The local hybrid systems that run the inference on consumer or clinic hardware, and the community screening tools that run on a device in the field, show that the edge deployment is not merely proposed but implemented, and their reports emphasise the privacy benefit of keeping the data local as the primary motivation.(6,8) The federated-learning framework in endodontics extends the same privacy logic to the training of the model, proposing that the models be trained across institutions without the images ever leaving each site, and this is the edge principle applied to the learning rather than the inference.(10)The adversarial-vulnerability study on panoramic segmentation is the cautionary counterpoint, showing that a model deployed at the edge inherits the vulnerabilities of the model it hosts, and that the edge does not, by itself, make the system secure.(11)Eleven studies in total bear on this axis when the federated and the adversarial evidence are included together, and the consistent message is that the edge is the right place for the inference and the wrong place to assume security.

The Internet of Things in dental care

The evidence on the Internet of Things describes an extension of the dental system beyond the clinic, and the dental literature on this axis is thinner than the edge-computing literature because the connected dental device is an earlier and more fragmented category. The Internet of Things devices that the wider literature describes, the sensors, the wearables and the smart patches, generate the continuous and in-situ data that the clinic-based examination cannot, and the dental-specific examples, the smart toothbrush and the intraoral sensor, belong squarely to this category.(12-14)The Internet of Medical Things extends the same logic to the clinic, connecting the imaging and the monitoring devices into a network that continuously feeds the artificial intelligence models, and the blockchain-based frameworks that the wider literature proposes are the response to the governance problem that this connectivity creates.(15,16) Seven studies support this axis directly, and they describe, in summary, a data-rich but governance-poor extension of the dental system into new settings.

The dental manifestations of the Internet of Things are earlier and more fragmented than the literature's maturity might suggest, and this fragmentation is itself a finding. The smart toothbrush, the intraoral sensor and the connected imaging device are the dental instances of a category that

is otherwise well developed in the medical domain, and the dental literature treats them as emerging rather than established, which reflects both the small scale of the dental device market and the absence of the interoperability standards that the wider Internet of Medical Things has begun to develop.(12,14) The consequence is that the dental connected device is adopted piecemeal, one product at a time, without the common security and governance layer that would make the piecemeal adoption safe, and this is the condition in which the security risk described below arises.

The connected dental device carries a specific risk that the wider Internet of Things literature names precisely, and it is the multiplication of the attack surface. Every connected sensor and every smart device is a potential point of entry for an attacker, and the intrusion-detection and the secure-authentication approaches that the wider literature develops are the response to that risk.(17-19)The dental-specific evidence on this particular risk is sparse, which is itself a finding, because the dental field has adopted the connected device more readily than it has adopted the security practice that the device requires, and the dentists' awareness studies confirm that the security dimension is under-recognised in the profession.(20,21) The patient-perspective and the public-health studies add the further point that the connected dental system raises expectations and questions that the profession is only beginning to articulate.(22,23) Eleven studies bear on this axis when the awareness and the perspective evidence are included together, and the consistent message is that the connectivity has arrived before the governance that should accompany it.

The data that the connected dental device produces is the reason its security matters, and the nature of that data deserves a word. The intraoral photograph, the radiograph and the longitudinal record of a patient's oral health are identifiable, sensitive and, in aggregate, more revealing than a single data point, because they describe a person's health, habits and even identity over time. The connected device that collects and transmits this data is therefore not a convenience with a security afterthought but a custodian of sensitive health information, and the review treats it as such throughout. This is the reason that the security axis is not optional but constitutive, and it is the reason the governance question, the question of who may access the data and under what conditions, is as important as the technical question of how the data is protected.

Cybersecurity threats and safeguards

The evidence on cybersecurity is the least mature of the three axes, and the dental-specific evidence is the thinnest of all, which is itself the review's most important negative finding. The wider medical-device-security literature is unambiguous that the connected medical device is a target, and that the risk is not hypothetical, and the modular risk-management and the zero-trust frameworks that it proposes are the safeguards that a dental deployment would need.(24-26)The security literature on the Internet of Things adds the specific threat models, the intrusion, the tampering and the privacy breach, and the artificial-intelligence-driven defences that it develops are a response to those models.(27-29)The adversarial-vulnerability study on dental radiographs is the single most direct piece of dental evidence on this axis, and it demonstrates that the models themselves, not merely the devices, are vulnerable.(11)The dental field therefore has the framework and the threat models readily available to it, but it has generated little evidence of its own on their application, and that specific gap is the axis's defining feature. Ten studies support this axis directly, and they converge on the conclusion that the safeguards exist while the dental evidence of their application does not yet.

The specific threats that a dental deployment faces are the same threats that the wider medical-device literature catalogues, and they can be stated concretely. The first is the adversarial attack on the model, in which a perturbed image causes a misclassification, and the dental adversarial-vulnerability study demonstrates that the panoramic segmentation models are susceptible to exactly this.(11)The second is the intrusion into the device or the network, in which a connected sensor or an imaging device is compromised to exfiltrate data or to corrupt the output, and the intrusion-detection literature supplies the defences that the dental field has not yet adopted.(17,18) The third is the privacy breach in the transfer of the data, and the federated and the encryption approaches are the response.(30,31) These three threats map onto the three axes of the review, and they are the reason the axes cannot be secured in isolation from one another.

The safeguards that the literature proposes are themselves a taxonomy, and it is worth laying them out so that the dental practitioner can see what is available. The preventive safeguards, the secure authentication and the encryption, protect the device and the transfer before an attack occurs, and the post-quantum and the blockchain-based frameworks are the more demanding instances of this class.(31,32) The detective safeguards, the intrusion-detection and the anomaly-detection models, identify an attack that has occurred, and the lightweight transformer and the

drift-aware detectors are the edge-appropriate instances.(17,18) The governance safeguards, the risk-management and the zero-trust frameworks, organise the whole into a defensible posture, and the modular frameworks that integrate the cybersecurity with the patient safety are the most complete instance.(24,25) The dental field has all three classes available to it, and the review's conclusion is that it has adopted the preventive class in the form of the local deployment while leaving the detective and the governance classes largely to the wider, non-dental literature.

The governance dimension completes the cybersecurity axis, and it is the part that the technical literature alone cannot address. The data-security and the ethical-awareness studies in dentistry document that the profession recognises the importance of data security without yet having the practices in place, and the patient-perspective studies show that the public's trust in the connected dental system is conditional on exactly those practices.(20,22) The blockchain and the post-quantum authentication frameworks of the wider literature are the technical answers to the governance question, and the simulation studies of differentially private federated learning are the bridge between the privacy of the data and the performance of the model.(30,31,33)The experimental protocols for secure healthcare artificial intelligence provide the template for how the dental field could generate the evidence it currently lacks.(34)Nine studies bear on the governance sub-axis, and they describe a ready set of tools that the dental field has not yet taken up in its own practice.

The remaining studies complete the picture with evidence on the enabling and the limiting factors. The software-development report documents how the dental tools themselves are now built with artificial intelligence assistance, and the survey of security and privacy issues in edge-assisted Internet of Things supplies the threat taxonomy that the dental field has not yet produced for itself.(9,35) The blockchain-based patient-centric framework and the FPGA-enabled smart implants represent the two ends of the connected-device spectrum, the governance layer and the device itself, and the educational-gaps study and the public-health-surveillance review situate the deployment within the workforce and the system that must adopt it.(36-39)Six studies support this enabling axis, and they converge on the conclusion that the tools and the devices exist while the workforce and the governance that would use them safely do not yet.

Deployment architectures

The evidence on deployment architectures synthesises the other three axes into a set of concrete, actionable choices, and it is the most actionable of the four axes. The hybrid local-cloud architecture, in which the inference runs locally and the more demanding computation or the model updates run in the cloud, is the architecture that the dental deployment literature consistently proposes, and it is the architecture that best reconciles the latency and privacy of the edge with the capacity of the cloud.(6,40) The federated-learning architecture extends the same reconciliation to the training of the model itself, and it is the answer to the multi-institution privacy problem that the dental repositories and the generalisation studies identify as a barrier to the field.(10,41,42)The blockchain-based approaches add a governance layer to the architecture, and the edge-IoT-security surveys describe the full stack within which these choices are made.(32,43,44)Seven studies support this axis directly, and they converge on the hybrid architecture and federated learning as the approaches that the dental field should now adopt.

The choice among the architectures is a choice among trade-offs, and the review's purpose is to make those trade-offs explicit rather than to prescribe a single answer. The hybrid architecture accepts the complexity of running two environments in exchange for the privacy of the local inference and the capacity of the cloud, and it is the choice that the dental deployment literature reaches when it weighs the compliance burden against the model performance.(6,40) The federated architecture accepts the complexity of the distributed training in exchange for keeping the data at its source, and it is the choice that the multi-institution generalisation problem requires.(10,41) The blockchain layer accepts the overhead of a distributed ledger in exchange for a tamper-evident record of the data's provenance, and it is the choice that the governance problem requires.(32,43) Each of these choices is a response to a specific requirement, and the practitioner who understands the requirements can choose accordingly.

The cloud-only and the local-only alternatives each fail one of the requirements, and the comparison is what makes the hybrid the consensus. The cloud-only architecture offers capacity but fails the privacy and the latency requirement, and the local-only architecture offers privacy but fails the capacity and the update requirement, and the dental deployment literature reaches the hybrid as the natural resolution of that opposition.(6,7,45)The federated-learning framework in endodontics and the differentially-private simulation are the concrete instances of how the hy-

brid and the federated principles are applied in the dental domain, and they are the most directly transferable evidence that the review can offer a practitioner.(10,30) The comprehensive dental repositories that the generalisation literature calls for are the exact data foundation that the federated architecture would need, and the two are therefore complementary rather than competing proposals.(41)Eleven studies bear on this axis when the repositories and the surveys are included all together, and the consistent message is that the architecture is a largely solved problem and the data and the governance are not yet.

DISCUSSION

The implication that the synthesis leads to is that the infrastructure of dental artificial intelligence is maturing faster than the security and the governance that its deployment requires, and this implication is the single most important conclusion of the review. The edge-computing and the deployment-architecture evidence is mature and convergent, and it tells a practitioner clearly where and how to run a dental model; the cybersecurity and the governance evidence is, by contrast, thin in the dental domain and borrowed largely from the wider medical-device literature, and it tells the practitioner that the safeguards exist but have not been validated in dentistry. The gap between the two is the risk that a connected dental system deployed today would carry, and the review's central message is that the field should close that gap deliberately before it deploys at scale. The maturity of the edge and the architecture evidence should not be mistaken for the maturity of the whole system, because a well-deployed model on an unsecured device is a liability, not an asset, and the review's emphasis on the gap is meant precisely to prevent that mistake.

The relationships between the axes are as important as the axes themselves, and they are what the thematic organisation is meant to reveal. Edge computing and the Internet of Things are in genuine tension, because every connected device that the Internet of Things adds is a device that the edge must secure, and the multiplication of devices that extends the data collection is also the multiplication of the attack surface.(27,28) Cybersecurity is therefore the constraint that the other two axes impose on each other, and the deployment architecture is the place where the three axes are reconciled into a single coherent system.(43,44) The federated-learning approach sits at the intersection of all four axes, because it addresses the privacy of the data, the distribution of the computation and the security of the transfer in a single integrated design, and this is the reason the review identifies it as the most promising single direction.(10,30)

The comparison with the wider medical-device and edge-computing literature is what gives the dental findings their context, and it is instructive in both directions. The dental field is ahead of the wider literature in one respect, which is the demonstrated enthusiasm for the local and the community deployment, and behind it in another, which is the generation of its own security evidence.(8,26) The wider literature has spent years building the frameworks and the taxonomies that the dental field has only begun to borrow, and the borrowing is visible in the way the dental deployment papers cite the medical-device-security literature rather than produce dental-specific counterparts.(24,25) This is not a criticism of the dental field, which is young in this respect, but a description of its position, and it is the position that the review's agenda is meant to move.

The cross-cutting gaps that the synthesis reveals are three, and they are stated as gaps rather than as limitations of the review. The first is the absence of dental-specific cybersecurity evidence, which the field borrows from the wider medical-device literature without validating it in the dental context, so that a dental practitioner must currently trust conclusions that were established in other specialties.(24,26) The second is the absence of the data foundation that the federated and the generalisable approaches require, the comprehensive repositories that the field has repeatedly identified as necessary but has not yet built.(41)The third is the awareness gap in the profession, documented directly in the dentist studies, which means that the technical safeguards, even where they exist, are not matched by the practices and the habits of the practitioners who would use them.(20,21) These three gaps together are the agenda that the review leaves for the field to address.

The agenda that the review leaves is as specific as the gaps are clear, and it can be stated in three items. The dental field needs its own security evidence, which means applying the threat models and the intrusion-detection and the adversarial-robustness methods to dental models and devices, rather than borrowing the conclusions from the wider medical-device literature.(11,24) It needs the data foundation that the federated and the generalisable approaches require, the comprehensive, privacy-preserving repositories that the field has identified as necessary but not yet built.(41)And it needs the professional awareness that the safeguards require, the education and the practice change documented as lacking in the dentist awareness studies.(20,38) These

three items follow directly from the three gaps, and they are stated as an agenda rather than as a general call for further research.

The implications for practice are the practical translation of the three axes, and they are stated concretely rather than as a general caution. A practitioner who deploys a dental model should choose the hybrid local-cloud architecture, keeping the inference and the identifiable data on site and reserving the cloud for the model updates and the non-identifiable computation, because that is the architecture that the evidence converges on.(6,40) A practitioner who adopts a connected dental device should assume that every device is a potential point of compromise and should require, before adoption, the security practices that the device's vendor can demonstrate, because the dental-specific security evidence is too thin to justify an assumption of safety.(20,27) And a practitioner who participates in a multi-institution initiative should prefer the federated approach, which keeps the data at its source, over the pooled approach, which concentrates the risk.(10,30) These three recommendations follow directly from the three axes and are the review's actionable content.

The recency of the evidence is itself a property of the field that the review must record, because it conditions every conclusion. The dental-specific studies of the three themes are, almost without exception, from 2026, and the wider edge-computing and security literature that the review borrows is likewise recent, so the synthesis describes a field at the very beginning of its deployment rather than a settled practice. This recency cuts both ways: it makes the review timely, because it captures the field at the moment the deployment questions first become urgent, and it makes the conclusions provisional, because the dental-specific security evidence that the review identifies as missing may well appear in the next few years. A reader who returns to these questions later will find a field that has either closed the gap the review describes or failed to, and the three axes identified here are the axes along which that progress, or its absence, should be measured.

Limitations

The limitations of this review follow from its narrative method and from the state of the evidence it reviews. The selection of studies was not systematic, and the dental-specific evidence on the cybersecurity axis is so thin that the review necessarily borrows heavily from the wider medical-device and edge-computing literature, which limits the directness of its conclusions for the dental practitioner.

The thematic grouping, while transparent, inevitably assigns studies to axes on the basis of the reviewer's judgement, and a study that addresses two axes is assigned to the one that it primarily addresses, with the cross-references noted where they matter. The absence of a dental-specific security evidence base is itself a genuine finding of the review, but it is also a limitation of the review, because it means the review's security conclusions are transferred from adjacent fields rather than established within dentistry itself.

CONCLUSIONS

Edge computing and the deployment architectures for dental artificial intelligence are mature and convergent, and the hybrid local-cloud architecture and federated learning are the approaches that best reconcile privacy with performance, while the Internet of Things extends the reach of the dental system into the home and the mouth and cybersecurity remains the least mature and the least dental-specific of the three determinants.

The three themes are one system, and the review's synthesis shows that the system's technical parts have matured ahead of its security and its governance, which is the condition in which a deployment is most at risk, because the capability exists before the safeguards that should accompany it. The infrastructure of dental artificial intelligence is therefore maturing faster than the security and the governance that its deployment requires, and the field must close that gap, through dental-specific security evidence, the data repositories that federated learning needs and the professional awareness that the safeguards require, before connected dental intelligence can be deployed at scale.

The infrastructure of dental artificial intelligence is therefore maturing faster than the security and the governance that its deployment requires, and the field must close that gap, through dental-specific security evidence, the data repositories that federated learning needs and the professional awareness that the safeguards require, before connected dental intelligence can be deployed at scale.

REFERENCES

1. Deng S, Zhao H, Fang W, Yin J, Dustdar S, Zomaya AY. Edge Intelligence: The Confluence of Edge Computing and Artificial Intelligence. IEEE Internet Things J. 2020;7(8):7457-7469. doi: 10.1109/jiot.2020.2984887
2. Xhafa F. Towards artificial intelligence internet of things (AIoT) and intelligent edge: The intelligent edge is where action is!. Internet of Things. 2023;22:100752. doi: 10.1016/j.iot.2023.100752
3. Kim G, Yoo S, Kang TW, Huang Y, Yeo W. Advances in Bio-Integrated Edge Computing Systems for Smart and Connected Health. Advanced Materials. 2026:e75390. doi: 10.1002/adma.75390
4. Kumar SS, Jerlin MA. Intelligent defense at the edge: a comprehensive survey of federated learning, TinyML and explainable AI for intrusion detection in IoT and IIoT ecosystems. Front Artif Intell. 2026;9:1900815. doi: 10.3389/frai.2026.1900815
5. Pawar S, Patil S, Sengar A, Khairnar K, Thite S, Israr M. SecureHealthKey+: Integrating Explainable TinyML Anomaly Detection Into Lightweight Authentication Protocols in IoT-Enabled Healthcare Systems. JoVE. 2026;(236). doi: 10.3791/73288
6. Sato M, Matsushita Y, Takahashi H, Kakazu T, Nagata S, Ohnuma M, et al. System Architecture of a Local Hybrid AI for Secure Patient Communication: Implementation on Consumer Hardware. In: Studies in Health Technology and Informatics. IOS Press; 2026. p. 534-538. doi: 10.3233/shti260228
7. Giannakis G. Towards an AI Powered Dental Clinic Management Ecosystem. In: Studies in Health Technology and Informatics. IOS Press; 2026. p. 353-357. doi: 10.3233/shti260862
8. Wongsapai M, Wudtijureepun K, Suthachai T, Tamdee D, Ittichaicharoen J, Wuttisarnwattana P, et al. A Community-Based Usability Study of an AI-Enabled Oral Cancer Screening App Operated by Village Health Volunteers: Mixed Methods Study. JMIR Mhealth Uhealth. 2026;14:e83738-e83738. doi: 10.2196/83738
9. Reymus M, Tichy A, Diegritz C, Weisbrod B, Schwendicke F, Werner N. AI-assisted software development in digital dentistry: A technical innovation report with three open-source applications. Journal of Dentistry. 2026;175:106864. doi: 10.1016/j.jdent.2026.106864
10. Turky M, Samaranayake L, Osathanon T, Dummer PMH. Federated Learning in Endodontics: A Framework for Privacy-Preserving Multicentre Artificial Intelligence. International Dental Journal. 2026;76(4):109704. doi: 10.1016/j.identj.2026.109704
11. Kohinoor MSR, Ahmed I, Shorfuzzaman M, Alam MS, Azzedin F, Rahman MM. Adversarial vulnerability and robustness of deep learning models for panoramic dental X-ray segmentation. Sci Rep. 2026;16(1):27704. doi: 10.1038/s41598-026-57108-x
12. Omiyale BO, Ogbeyemi A, Odeyemi J, Ashraf MA, Olugbade TO, Song KY, et al. Recent advances in smart nanosensors and IoT-based systems for real-time diagnostic monitoring. Anal Methods. 2026;18(34):7208-7253. doi: 10.1039/d6ay01081d
13. Umapathi K, Priya L, Fayek HH. Smart patches for healthcare industry: a review of emerging technologies, challenges, and developmental opportunities. BioMed Eng OnLine. 2026;25(1):23. doi: 10.1186/s12938-025-01485-3
14. Aziz A, Kaçmaz S, Aladwani AIA. Artificial Intelligence-Enabled Medical Diagnosis in the Internet of Medical Things: An End-to-End Survey of Connected Sensing, Distributed Intelligence, Clinical Applications, and Validation. Diagnostics. 2026;16(19):3171. doi: 10.3390/diagnostics16193171
15. Di Grezia G, Clemente A, Dugheri S, Mattei V, Gili A, Mari E, et al. Blockchain and Internet of Medical Things for Resilient Healthcare. Bioengineering. 2026;13(10):1173. doi: 10.3390/bioengineering13101173
16. Yaghobian S, Sulkowski N, Galambos G, Scarazzini L, Maloumian N, Verhaeghe S. Blockchain for Digital Health Governance: Evidence Gap Map and Scoping Review. J Med Internet Res. 2026;28:e96098-e96098. doi: 10.2196/96098
17. Alhafi D, Alanazi F. CyberRoBERTa: A Lightweight Transformer-Based Language Model for IoT Intrusion Detection. Sensors. 2026;26(19):6326. doi: 10.3390/s26196326
18. Günay B, Yağcı MY. DEA-IDS: Drift-Aware Feature Selection and Few-Shot Adaptation for Cross-Domain IoT–IoMT Intrusion Detection. Sensors. 2026;26(19):6200. doi: 10.3390/s26196200
19. Gong Z, Xiong N, Zhao C, Chen J, Ammar O, Shaikh JA, et al. FedLC-Trans: privacy-preserving CNN–Transformer fusion for resilient IoMT intrusion detection. Front Public Health. 2026;14:1924540. doi: 10.3389/fpubh.2026.1924540
20. Ozbey F, Gokkurt Yilmaz BN, Yilmaz BE. Dentists' awareness of data security and ethical issues during the transition to artificial intelligence-driven clinical practice. AOS. 2026;85:61-66. doi: 10.2340/aos.v85.45419
21. Efthymiou G, Charalambous M, Soteriades ES. Dentists', dental students' and patients' knowledge, attitudes and practices on artificial intelligence: a scoping review. BMC Oral Health. 2026;26(1):1765. doi: 10.1186/s12903-026-09081-0
22. Cozmescu AF, Cernega A, Didilescu AC, Imre MM, Funieru C, Pițuru SM. Patients' Perspectives on Artificial Intelligence and Digital Transformation in Dental Practice: A Cross-Sectional Study from Romania. Dent J. 2026;14(9):572. doi: 10.3390/dj14090572
23. Madhumitha S, Thippeswamy HM, Gade VC. Integration of artificial intelligence in public health dentistry: applications, challenges, and future directions — a scoping review. Saudi Dent J. 2026;38(9):112. doi: 10.1007/s44445-026-00221-4
24. Pohjosaho P, Mikkonen T, Stefanidis K, Stirbu V, Granlund T. A modular risk management framework for integrating cybersecurity and patient safety in medical device software development. Front Digit Health. 2026;8:1903787. doi: 10.3389/fdgth.2026.1903787
25. Oke F. Operationalizing clinical artificial intelligence through secure FHIR pipelines: a zero-trust cloud reference architecture for EHR interoperability. Front Digit Health. 2026;8:1953969. doi: 10.3389/fdgth.2026.1953969

26. Goh CJ, Liu H, Devendra N, Cao KN. Cybersecurity of Large Language Models Across the Deployment Life Cycle in Health Systems. JMIR Med Inform. 2026;14:e101715. doi: 10.2196/101715
27. Khokhar E, Irshad Ahmed. Cybersecurity Challenges, Vulnerabilities, and Emerging Security Solutions in the Internet of Things. JAIC. 2026;4(1):1-7. doi: 10.57041/jjfgdk93
28. Abed AK, Anupam A. Review of security issues in Internet of Things and artificial intelligence-driven solutions. Security and Privacy. 2023;6(3):e285. doi: 10.1002/spy2.285
29. Kuzlu M, Fair C, Guler O. Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity. Discov Internet Things. 2021;1(1):7. doi: 10.1007/s43926-020-00001-4
30. Masad IS, Alqudah AM, Qazan S, Shoaib S. A simulation study of differentially private federated learning with zero-trust policy screening for medical IoT devices. Front Digit Health. 2026;8:1807342. doi: 10.3389/fdgth.2026.1807342
31. Shen W, Mo J, Lin Y. An Efficient Post-Quantum User Authentication Protocol for Wireless Sensor Networks Using NTRU. Entropy. 2026;28(10):1049. doi: 10.3390/e28101049
32. Assistant Professor, Ch. Bansilal University, Bhiwani, Haryana, Priyanka D. Edge Computing-Assisted Internet of Things: A Blockchain-Based Approach to Security and Privacy Concerns. ETJ. 2026;11(02). doi: 10.47191/etj/v11i02.04
33. Ferreira JC, Esperança M, Freitas D, Botas J, Mataloto B, Bezerra R, et al. IoT2Wallets: A Blockchain-Based Access Control and Consent-Auditing Architecture for Patient-Controlled Health IoT Data Integration. Sensors. 2026;26(20):6658. doi: 10.3390/s26206658
34. Patil S, Lokhande M, Koparde S, Kothari S, Jha S. Experimental Protocols for Developing and Validating Explainable AI Models in Secure Healthcare Diagnostics. JoVE. 2026;(236). doi: 10.3791/72412
35. Alwarafy A, Al-Thelaya KA, Abdallah M, Schneider J, Hamdi M. A Survey on Security and Privacy Issues in Edge-Computing-Assisted Internet of Things. IEEE Internet Things J. 2021;8(6):4004-4022. doi: 10.1109/jiot.2020.3015432
36. Sawant NM, Gomes J. Patient-Centric Blockchain-Enabled Framework for Secure Medical Data Sharing in Indian EHR Systems. Crit Rev Biomed Eng. 2026;54(3):21-46. doi: 10.1615/critrevbiomedeng.2026059613
37. Strydis C, Veselka D, van der Kleij J, Siddiqi MA. FPGA-Enabled, Smart Implants: A Path to Personalized Healthcare. IEEE Open J Eng Med Biol. 2026;7:291-300. doi: 10.1109/ojemb.2026.3720369
38. Ela H, Moustapha R, Badran A, Abou-Bakr A, Almalahy H. Educational gaps and factors associated with artificial intelligence adoption among Egyptian periodontists: a multicenter cross-sectional study. Sci Rep. 2026;16(1). doi: 10.1038/s41598-026-65434-3
39. Khobragade R, Shaikh M, Mendhe H, Borkar S, Gurdekar A, Shendre S, et al. Role of Digital Health Technologies and Artificial Intelligence in Modern Public Health Surveillance. Cureus. 2026;18(4):e106690. doi: 10.7759/cureus.106690
40. Wang Z, Kapri N, Bittencourt LF, Buyya R. Artificial intelligence-driven resource management in edge-cloud computing continuum for internet of things applications: new trends and future directions. Front Internet Things. 2026;5:1883673. doi: 10.3389/friot.2026.1883673
41. Thakkar S, Flores M, Singh B, Khan A. The Fundamental Necessities of Comprehensive Dental Repositories to Support the Generalisation of AI Applications in Endodontics. Int Endodontic J. 2026:iej.70286. doi: 10.1111/iej.70286
42. Li H, Ge L, Tian L. Survey: federated learning data security and privacy-preserving in edge-Internet of Things. Artif Intell Rev. 2024;57(5):130. doi: 10.1007/s10462-024-10774-7
43. Muhati E, Rawat DB, Sadler BM. A New Cyber-Alliance of Artificial Intelligence, Internet of Things, Blockchain, and Edge Computing. IEEE Internet Things M. 2022;5(1):104-107. doi: 10.1109/iotm.001.2100181
44. Rupanetti D, Kaabouch N. Combining Edge Computing-Assisted Internet of Things Security with Artificial Intelligence: Applications, Challenges, and Opportunities. Applied Sciences. 2024;14(16):7104. doi: 10.3390/app14167104
45. Wang C, Yuan Z, Zhou P, Xu Z, Li R, Wu DO. The Security and Privacy of Mobile-Edge Computing: An Artificial Intelligence Perspective. IEEE Internet Things J. 2023;10(24):22008-22032. doi: 10.1109/jiot.2023.3304318

FUNDING

No financing

CONFLICT OF INTEREST

None

AUTHORSHIP CONTRIBUTIONS

Drafting – original draft: Diana Anselmo, Stacey Estefan.
Writing–review and editing: Diana Anselmo, Stacey Estefan.