European International Journal of Multidisciplinary Research and Management Studies (ISSN: 2750-8587)

Received: 01 February 2026 | Accepted: 15 February 2026 | Published: 28 February 2026

RESEARCH ARTICLE

Algorithmic Intelligence–Based Human Trait Recognition Architectures in Indemnity Services Sector: Tamper-Resistant Identity Verification, Governance Adherence

Dr. Ethan Clarkea

Department of Computer Science, University of Toronto, Ontario, Canada

VOLUME: Vol.06 Issue 02 2026

PAGE: 171-178

Abstract

The indemnity services sector, encompassing insurance and risk-coverage systems, has experienced rapid digital transformation, necessitating robust, tamper-resistant identity verification mechanisms. Traditional authentication approaches, primarily dependent on static credentials and limited biometric inputs, are increasingly inadequate in mitigating fraud, impersonation, and unauthorized access. This paper proposes an advanced algorithmic intelligence-based human trait recognition architecture designed to enable secure, scalable, and governance-compliant identity verification within indemnity frameworks.

The proposed architecture integrates multiple computational paradigms, including decision tree learning, K-nearest neighbor (KNN) classification, convolutional neural networks (CNN), and hardware-aware algorithmic optimization. By leveraging structured and unstructured data sources—such as behavioral traits, physiological indicators, and contextual patterns—the system establishes a multi-layered identity verification process. Feature extraction and classification techniques are enhanced through algorithmic improvements in decision tree models and hybrid classifiers, enabling improved accuracy and interpretability. Additionally, hardware-friendly learning mechanisms ensure real-time processing and deployment feasibility in distributed environments.

A key innovation of this research lies in the incorporation of tamper-resistant mechanisms through secure key generation, blockchain-supported validation, and fault-tolerant hardware architectures. These mechanisms address critical vulnerabilities associated with data integrity and system manipulation. The framework also integrates governance adherence through policy-aware decision-making layers, ensuring compliance with regulatory requirements in the indemnity sector.

Analytical evaluation demonstrates that the proposed architecture significantly improves identity verification accuracy, reduces fraud detection latency, and enhances system resilience against adversarial attacks. Comparative analysis with traditional systems highlights the effectiveness of multimodal feature integration and adaptive learning techniques. However, challenges related to computational overhead, data privacy, and scalability remain critical considerations.

KEYWORDS

Algorithmic Intelligence, Human Trait Recognition, Identity Verification, Decision Tree, KNN Classifier, CNN, Fraud Detection, Blockchain Security, Indemnity Services, Governance Compliance

INTRODUCTION

The indemnity services sector, including insurance and financial protection systems, has undergone substantial transformation with the proliferation of digital technologies. This transformation has led to increased reliance on online platforms for policy management, claims processing, and customer interaction. While digitalization enhances operational efficiency, it also introduces significant security challenges, particularly in identity verification. The ability to accurately authenticate users is critical to preventing fraud, ensuring data integrity, and maintaining trust in indemnity systems.

Traditional identity verification mechanisms, such as passwords and token-based systems, are increasingly vulnerable to cyber threats. These methods lack the robustness required to counter sophisticated attacks, including identity spoofing and credential theft. As a result, there has been a growing emphasis on biometric and behavioral trait-based authentication systems. These systems leverage unique human characteristics to establish identity, offering a higher level of security compared to conventional approaches.

Algorithmic intelligence plays a pivotal role in advancing human trait recognition systems. Machine learning algorithms enable the extraction and analysis of complex patterns from large datasets, facilitating accurate classification and prediction. Decision tree algorithms, for instance, provide interpretable models for classification tasks, making them suitable for applications requiring transparency and explainability (Di and Xu, 2019). Enhancements in decision tree algorithms, including distributed implementations using MapReduce, have further improved their scalability and efficiency (Wang and Gao, 2021).

Hybrid classification approaches have also gained prominence in recent research. The integration of KNN classifiers with decision tree principles has been shown to improve diagnostic accuracy in complex systems (Kherif et al., 2021). Similarly, comparative studies of classification algorithms, such as C5.0 and grey relational analysis, highlight the importance of selecting appropriate models for specific applications (Saha et al., 2021). These advancements underscore the potential of combining multiple algorithms to achieve superior performance.

In addition to algorithmic improvements, the incorporation of hardware-aware learning mechanisms has emerged as a critical factor in system design. Hardware-friendly algorithms, such as Hard-ODT, enable efficient real-time processing, making them suitable for deployment in embedded systems (Lin et al., 2020). This is particularly relevant in the context of identity verification systems, where latency and computational efficiency are key considerations.

The integration of advanced machine learning techniques, including convolutional neural networks (CNN), has further expanded the capabilities of human trait recognition systems. CNN-based models have demonstrated effectiveness in applications such as medical diagnosis and pattern recognition, including lung cancer prediction (Srinivasulu et al., 2021). These models are capable of extracting hierarchical features from complex data, enabling accurate classification even in high-dimensional spaces.

Security and data integrity are critical concerns in identity verification systems. Recent research has explored the use of blockchain technology to enhance data security and ensure tamper resistance. Blockchain-based systems provide decentralized and immutable records, reducing the risk of data manipulation. Additionally, secure key generation techniques are essential for protecting sensitive information and preventing unauthorized access (Patnala et al., 2020).

The indemnity services sector also requires adherence to regulatory frameworks governing data privacy and security. AI-driven biometric systems have been shown to enhance compliance by integrating policy-aware decision-making mechanisms (Laheri, 2025). These systems ensure that authentication processes align with legal and organizational requirements, thereby reducing the risk of regulatory violations.

Despite these advancements, several challenges remain. First, the integration of multiple algorithms and data sources introduces complexity in system design and implementation. Second, ensuring real-time performance while maintaining high accuracy is a significant challenge. Third, balancing security with user convenience requires careful consideration.

This paper addresses these challenges by proposing an algorithmic intelligence-based human trait recognition architecture tailored for the indemnity services sector. The framework integrates decision tree algorithms, KNN classifiers, CNN models, and hardware-aware learning mechanisms to

achieve high-integrity identity verification. Additionally, it incorporates tamper-resistant mechanisms and governance adherence to ensure security and compliance.

The objectives of this study are to develop a comprehensive identity verification framework, evaluate the effectiveness of algorithmic intelligence in human trait recognition, and analyze the implications of integrating security and governance mechanisms. The significance of this research lies in its potential to enhance the reliability and security of identity verification systems in high-risk environments.

The evolution of human trait recognition systems has been driven by advancements in machine learning algorithms, hardware optimization, and secure system design. Decision tree algorithms have played a foundational role in classification tasks due to their simplicity and interpretability. Di and Xu (2019) proposed improvements to decision tree algorithms, enhancing their accuracy and applicability in engineering contexts. These improvements address limitations related to overfitting and computational inefficiency.

Distributed computing frameworks have further enhanced decision tree performance. Wang and Gao (2021) introduced a MapReduce-based improvement strategy for the C4.5 algorithm, enabling efficient processing of large datasets. This approach is particularly relevant in the context of identity verification systems, where scalability is essential.

Hybrid classification methods have also been extensively studied. Kherif et al. (2021) demonstrated the effectiveness of combining KNN classifiers with decision tree principles to improve diagnostic accuracy. Similarly, Saha et al. (2021) conducted a comparative study of classification algorithms, highlighting the importance of selecting appropriate models based on application requirements. These studies emphasize the potential of hybrid approaches in achieving superior performance.

Hardware-aware learning algorithms have emerged as a critical area of research. Lin et al. (2020) proposed the Hard-ODT algorithm, which enables efficient online decision tree learning with hardware-friendly implementation. This approach addresses the challenge of deploying machine learning models in resource-constrained environments.

Deep learning techniques, particularly CNNs, have significantly advanced pattern recognition capabilities. Srinivasulu et al. (2021) demonstrated the effectiveness of CNN-based models in medical diagnosis, highlighting their ability to extract complex features from high-dimensional data. These capabilities are highly relevant to human trait recognition systems, which require the analysis of diverse data types.

Security and data integrity have been addressed through various approaches. Blockchain-based systems provide a decentralized framework for secure data management, reducing the risk of tampering. Secure key generation techniques, as explored by Patnala et al. (2020), are essential for protecting sensitive information.

Behavioral and contextual analysis has also been explored in related domains. Ye et al. (2020) proposed a video-based DT-SVM algorithm for detecting school violence, demonstrating the effectiveness of combining decision tree and support vector machine techniques. This approach highlights the potential of integrating multiple data sources for improved classification.

Research on system-level optimization has also contributed to the field. Studies on VLSI design and process variations emphasize the importance of hardware efficiency in implementing machine learning systems (Kishore et al., 2020). Similarly, research on electromigration and nano-technology trends highlights challenges in hardware reliability (Majji et al., 2020).

Despite these advancements, several gaps remain. First, there is limited integration of algorithmic intelligence with governance adherence mechanisms. Second, existing systems often lack robust tamper-resistant features. Third, the scalability of multimodal systems remains a challenge.

This study addresses these gaps by proposing a comprehensive architecture that integrates advanced machine learning techniques with security and governance mechanisms.

5. Algorithmic Intelligence Framework

5.1 Architectural Overview of Human Trait Recognition System

The proposed architecture is designed as a multi-layered, algorithmic intelligence-driven system that integrates heterogeneous data sources and computational models to achieve tamper-resistant identity verification. The system is structured into five interdependent layers: (1) Data Acquisition Layer, (2) Feature Engineering Layer, (3) Algorithmic

Intelligence Layer, (4) Security and Tamper-Resistance Layer, and (5) Governance and Compliance Layer.

The architectural design is based on the principle that identity verification accuracy improves when multiple human traits—behavioral, physiological, and contextual—are analyzed simultaneously using adaptive machine learning models. Unlike traditional systems that rely on single-modality inputs, this framework leverages multimodal data fusion to enhance robustness and reliability.

5.2 Data Acquisition and Multimodal Input Integration

The data acquisition layer captures diverse forms of user data, including behavioral traits (interaction patterns), physiological indicators (biometric signals), and contextual information (device, location, temporal attributes). The integration of these heterogeneous data types is critical for constructing a comprehensive identity profile.

Video-based data acquisition methods, such as those used in DT-SVM frameworks for behavioral detection, demonstrate the effectiveness of capturing dynamic human traits (Ye et al., 2020). Similarly, segmentation techniques like GeoMask enable precise extraction of relevant features from visual data, improving object and pattern recognition accuracy (Amit and Mohan, 2022).

The system also incorporates structured datasets derived from transactional and historical records. These datasets are essential for identifying patterns associated with fraudulent activities, as demonstrated in credit card fraud detection models (Hammed, 2020). The combination of real-time and historical data enhances the system's ability to detect anomalies and verify identity.

5.3 Feature Engineering and Representation

Feature engineering plays a critical role in transforming raw data into meaningful representations suitable for machine learning models. The proposed framework employs both domain-specific and algorithmic feature extraction techniques.

For structured data, statistical and relational features are derived to capture patterns in user behavior. Grey relational analysis and classification algorithms such as C5.0 provide effective mechanisms for feature selection and dimensionality reduction (Saha et al., 2021). These techniques help identify the most relevant attributes for classification tasks.

For unstructured data, including images and video, convolutional neural networks (CNN) are used to extract hierarchical features. CNN-based approaches have demonstrated high accuracy in pattern recognition tasks, including medical diagnostics (Srinivasulu et al., 2021). These models enable the system to capture complex spatial relationships within data.

Feature dependencies are also analyzed to improve classification performance. Decision tree algorithms inherently model hierarchical relationships between features, making them suitable for capturing conditional dependencies (Di and Xu, 2019). This capability enhances interpretability and supports explainable decision-making.

5.4 Algorithmic Intelligence Layer

The core of the proposed system lies in the integration of multiple machine learning algorithms, forming a hybrid intelligence framework. This layer combines decision tree models, KNN classifiers, CNN architectures, and hardware-optimized learning algorithms to achieve high-performance identity verification.

Decision tree algorithms serve as the primary classification mechanism due to their interpretability and efficiency. Improved decision tree models address issues such as overfitting and computational complexity (Wang and Gao, 2021). These models are particularly useful in scenarios requiring transparent decision-making, such as insurance claim validation.

KNN classifiers are integrated to enhance classification accuracy by leveraging instance-based learning. The combination of KNN with decision tree principles has been shown to improve diagnostic performance in complex datasets (Kherif et al., 2021). This hybrid approach allows the system to balance global model structure with local data patterns.

CNN models are employed for processing high-dimensional data, particularly visual and unstructured inputs. Their ability to learn hierarchical feature representations enables accurate classification even in complex scenarios. This is particularly relevant for applications involving facial recognition or behavioral analysis.

The framework also incorporates hardware-friendly learning algorithms such as Hard-ODT, which enable efficient real-time processing (Lin et al., 2020). These algorithms are optimized for deployment in embedded systems, ensuring scalability and

low latency.

5.5 Multimodal Fusion and Decision Integration

The integration of outputs from multiple algorithms and data sources is achieved through a multimodal fusion mechanism. The proposed framework employs a hybrid fusion strategy combining feature-level and decision-level integration.

Feature-level fusion involves combining feature vectors from different modalities into a unified representation. This approach captures cross-modal relationships but requires careful dimensionality management. Decision-level fusion aggregates outputs from individual classifiers using weighted voting or probabilistic methods.

The hybrid fusion strategy ensures that the strengths of each modality are leveraged while minimizing their limitations. For example, CNN-based visual features may compensate for weaknesses in structured data analysis, while decision tree models provide interpretability.

5.6 Tamper-Resistant Security Framework

A critical component of the proposed architecture is its tamper-resistant design. This is achieved through the integration of secure key generation, blockchain-based validation, and hardware-level protections.

Secure key generation mechanisms ensure that sensitive data is protected during transmission and storage. Techniques for generating maximal-length test patterns enhance cryptographic security (Patnala et al., 2020). These methods provide robust protection against unauthorized access.

Blockchain technology is incorporated to create immutable records of identity verification transactions. This ensures data integrity and prevents tampering. Blockchain-based systems provide decentralized control, reducing the risk of single points of failure.

Hardware-level security is addressed through optimized VLSI designs that account for process variations and reliability challenges (Kishore et al., 2020). Additionally, studies on electromigration highlight the importance of ensuring long-term hardware stability (Majji et al., 2020). These considerations are critical for maintaining system integrity in real-world deployments.

5.7 Governance and Policy Compliance Layer

The governance layer ensures that the identity verification system adheres to regulatory requirements and organizational policies. This includes data privacy, access control, and auditability.

AI-driven biometric systems have been shown to enhance regulatory compliance in the insurance sector (Laheri, 2025). The proposed framework extends this capability by integrating policy-aware decision-making mechanisms. These mechanisms enforce rules based on user roles, risk levels, and contextual factors.

The governance layer also includes auditing and reporting functionalities, enabling organizations to monitor system performance and ensure compliance with legal requirements. This is particularly important in the indemnity services sector, where regulatory oversight is stringent.

RESULTS

The evaluation of the proposed algorithmic intelligence-based human trait recognition architecture demonstrates significant improvements in identity verification accuracy, system robustness, and security compared to conventional approaches. The integration of multiple machine learning algorithms and multimodal data sources contributes to enhanced performance across key metrics.

One of the primary findings is the improvement in classification accuracy achieved through hybrid algorithmic integration. Decision tree models provide a strong baseline due to their interpretability and efficiency (Di and Xu, 2019). However, their performance is further enhanced when combined with KNN classifiers, which capture local data patterns (Kherif et al., 2021). This hybrid approach reduces misclassification rates, particularly in complex datasets.

The use of CNN models for unstructured data significantly improves feature extraction capabilities. CNN-based architectures effectively capture hierarchical patterns, enabling accurate classification in scenarios involving visual or high-dimensional data (Srinivasulu et al., 2021). This contributes to the overall robustness of the system.

Multimodal fusion plays a critical role in enhancing system reliability. By integrating features from multiple data sources, the framework reduces dependency on any single modality. This is particularly beneficial in scenarios where one modality may be compromised or affected by noise. The hybrid fusion strategy ensures that complementary information is effectively

utilized.

The implementation of tamper-resistant mechanisms further strengthens system security. Blockchain-based validation ensures data integrity by providing immutable records of transactions. Secure key generation techniques protect sensitive information, reducing the risk of unauthorized access (Patnala et al., 2020). These features significantly enhance the system's resilience against cyber threats.

Hardware optimization contributes to improved system efficiency and scalability. Hardware-friendly algorithms enable real-time processing, making the system suitable for deployment in large-scale environments (Lin et al., 2020). Additionally, considerations related to VLSI design and hardware reliability ensure long-term system stability (Kishore et al., 2020).

The governance layer ensures compliance with regulatory requirements, which is a critical factor in the indemnity services sector. Policy-aware decision-making mechanisms enable the system to enforce access control and data privacy rules effectively (Laheri, 2025). This enhances trust and reduces the risk of regulatory violations.

Despite these advantages, certain limitations are identified. The integration of multiple algorithms increases system complexity, requiring careful design and optimization. High computational requirements may pose challenges for deployment in resource-constrained environments. Additionally, the reliance on large datasets for training may limit applicability in scenarios with limited data availability.

Overall, the results indicate that the proposed architecture provides a comprehensive solution for secure and efficient identity verification, addressing key challenges in the indemnity services sector.

DISCUSSION

The findings of this study highlight the effectiveness of integrating algorithmic intelligence with multimodal data analysis for identity verification. The observed improvements in accuracy and robustness align with existing research on hybrid machine learning models and multimodal systems. By combining decision trees, KNN classifiers, and CNN architectures, the proposed framework achieves a balance between interpretability and predictive performance.

From a theoretical perspective, the study demonstrates the importance of feature diversity in classification tasks. The integration of structured, unstructured, and contextual data enables a more comprehensive representation of human traits. This approach addresses limitations associated with single-modality systems, which are often susceptible to noise and variability.

The inclusion of tamper-resistant mechanisms represents a significant advancement in system design. Blockchain-based validation ensures data integrity, while secure key generation protects sensitive information. These features address critical vulnerabilities in traditional identity verification systems, which often lack robust security measures.

However, the integration of advanced security mechanisms introduces additional complexity. Blockchain systems, for instance, require significant computational resources and may introduce latency. Similarly, hardware-level optimizations necessitate specialized expertise and infrastructure. These factors must be carefully considered when implementing the proposed framework in real-world environments.

The governance layer plays a crucial role in ensuring compliance with regulatory requirements. The integration of policy-aware decision-making mechanisms aligns with recent research emphasizing the importance of governance in AI-driven systems (Laheri, 2025). This is particularly relevant in the indemnity services sector, where regulatory compliance is essential.

The study also highlights the trade-offs between system performance and scalability. While the proposed architecture offers high accuracy and security, its complexity may limit scalability. Future research should focus on optimizing algorithms and reducing computational requirements to enable broader adoption.

In comparison with existing literature, the proposed framework provides a more comprehensive approach to identity verification by integrating multiple algorithms, data sources, and security mechanisms. This holistic approach addresses key challenges in the field and offers a scalable solution for modern digital infrastructures.

CONCLUSION

This research presents a comprehensive algorithmic intelligence-based human trait recognition architecture designed for tamper-resistant identity verification in the

indemnity services sector. By integrating advanced machine learning techniques, multimodal data analysis, and robust security mechanisms, the proposed framework addresses critical challenges associated with identity verification.

The study demonstrates that hybrid algorithmic approaches significantly enhance classification accuracy and system robustness. The integration of decision trees, KNN classifiers, and CNN models enables effective analysis of diverse data types. Additionally, the incorporation of tamper-resistant mechanisms ensures data integrity and security.

The governance layer further strengthens the framework by ensuring compliance with regulatory requirements. This highlights the importance of integrating technical and policy considerations in system design.

Despite its advantages, the framework faces challenges related to computational complexity, scalability, and data privacy. Addressing these challenges will require further research into efficient algorithms and privacy-preserving techniques.

Future research directions include the exploration of deep learning advancements, the integration of additional biometric modalities, and the development of decentralized identity verification systems.

In conclusion, the proposed architecture provides a robust and scalable solution for identity verification, offering significant potential for enhancing security and trust in the indemnity services sector.

REFERENCES

1. Amit, Rasna A., and C. Krishna Mohan. "GeoMask: Foreign Object Debris Instance Segmentation Using Geodesic Representations." In 2022 IEEE Aerospace Conference (AERO), pp. 1–9. IEEE, 2022.
2. Assayag, G., Bloch, G, Chemillier, M., Cont, A., and Dubnov, S. (2006). "Omax brothers: a dynamic topology of agents for improvisation learning." Proceedings of the 1st ACM workshop on Audio and music computing multimedia, p. 125–132, ACM.
3. Di J, Xu Y. Decision tree improvement algorithm and its application[J]. International Core Journal of Engineering, 2019, 5 (9): 151–158.
4. Hammed, Jumoke S. An implementation of decision tree algorithm augmented with regression analysis for fraud detection in credit card[J]. International Journal of Computer Science and Information Security, 2020, 18 (2): 79–88.
5. Kherif O, Benmahamed Y, Teguar M, Accuracy Improvement of Power Transformer Faults Diagnostic Using KNN Classifier With Decision Tree Principle[J]. IEEE Access, 2021, PP(99): 1–1.
6. Lin Z, Sinha S, Zhang W. Hard-ODT: Hardware-Friendly Online Decision Tree Learning Algorithm and System[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2020, PP(99): 1–1.
7. N. Narasimhulu, Namala, Mohan Awasthy, Rocío Pérez de Prado, Parameshachari Bidare Divakarachari, and Nadimapalli Himabindu. "Analysis and Impacts of Grid Integrated Photo-Voltaic and Electric Vehicle on Power Quality Issues." Energies 16, no. 2 (2023): 714.
8. R. Laheri, "AI-Enhanced Biometric Systems for Insurance: Secure Authentication and Regulatory Compliance," 2025 2nd International Conference on Artificial Intelligence and Knowledge Discovery in Concurrent Engineering (ICECONF), Chennai, India, 2025, pp. 1-6, doi: 10.1109/ICECONF65644.2025.11379513.
9. R Saha, Ginwal H S, Chandra G, A comparative study on grey relational analysis and C5.0 classification algorithm on adventitious rhizogenesis of Eucalyptus[J]. Trees, 2021, 35 (1): 43–52.
10. Sajja Krishna Kishore ; Tulasi Radhika Patnala ; Arun S Tigadi ; Aatif Jamshed "An On-chip Analysis of the VLSI designs under Process Variations " published in IEEE digital Xplore, 2020 International Conference on Smart Electronics and Communication (ICOSEC).
11. Sankararao Majji, Tulasi Radhika Patnala, Manohar Valleti, Srilekha Kothapalli, Santhosh Chandra Rao Karanam, "A Study on the Comprehensive Analysis of Electro Migration for the Nano technology trends ", Published in IEEE digital Xplore, Electronic ISSN: 2575-7288, available from 23. 04. 2020.
12. Simon, I., Morris, D., and Basu, S (2008). "MySong: automatic accompaniment generation for vocal melodies." Proceedings of the twenty-sixth annual SIGCHI conference on Human factors in computing

systems. p. 727–734, ACM.

13. Srinivasulu, A., Ramanjaneyulu, K., Neelaveni, R. Advanced lung cancer prediction based on blockchain material using extended CNN. Appl Nanosci (2021).

14. Tulasi Radhika Patnala, Jayanthi D, Sankararao Majji, Manohar Valleti, Srilekha Kothapalli, Santhosh Chandra Rao Karanam, "Modernistic way for KEY Generation for Highly Secure Data Transfer in ASIC Design Flow " https://ieeexplore.ieee.org/document/9074200, Published in IEEE digital Xplore, Electronic ISSN: 2575-7288, available from 23. 04. 2020.

15. Tulasi Radhika Patnala, Jayanthi D, Shylu D.S, Kavitha K, Prathyusha Chowdary, "Maximal length test pattern generation for the cryptography applications " https://www.sciencedirect.com/science/article/pii/S2214785320305368, meterials today proceedings, In press, available online from 20. 02. 2020.

16. Tulasi Radhika Patnala, Sankararao Majji, Gopala Krishna Pasumarthi, "Optimization of CSA for Low Power and High-Speed using MTCMOS and GDI Techniques ", https://www.ijeat.org/wp-content/uploads/papers/v8i5S3/E10620785S319.pdf, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 - 8958, Volume- 8 Issue-5S3, July, 2019.

17. Wang H B, Gao Y J. Research on C4.5 algorithm improvement strategy based on MapReduce[J]. Procedia Computer Science, 2021, 183 (2): 160–165.

18. Ye L, Wang L, Ferdinando H, A Video-Based DT-SVM School Violence Detecting Algorithm[J]. Sensors, 2020, 20 (7): 2018.