ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753|| ISI Value: 1.188

FORMULATION AND EXECUTION OF A HYBRID ENCRYPTION ALGORITHM AND ACKNOWLEDGMENT PROTOCOL FOR SECURING THE DISTRIBUTION OF DATA

Dr. Madhu P
Guest Lecturer, Dept of Computer Science, Govt First Grade college, Hosadurga

Article DOI: https://doi.org/10.36713/epra28895
DOI No: 10.36713/epra28895

ABSTRACT

This research focuses on the formulation and execution of a novel Hybrid Encryption Algorithm, complemented by a robust acknowledgment Protocol, aimed at enhancing the security of data distribution. In response to the escalating threats to sensitive information during transmission, the proposed hybrid encryption algorithm amalgamates the strengths of symmetric and asymmetric cryptographic techniques. The synergistic approach ensures a formidable defense against potential security breaches. Furthermore, the accompanying acknowledgment protocol provides an additional layer of security by confirming successful data receipt, thereby mitigating the risks associated with data interception and unauthorized access. The comprehensive integration of these components establishes a resilient framework for securing the distribution of data, making it an instrumental contribution to the field of information security and cryptography.

1. INTRODUCTION

In today's digital landscape, the security and confidentiality of data have become paramount concerns due to the increasing prevalence of cyber threats and unauthorized access. As organizations and individuals exchange sensitive information over various communication channels, the need for robust encryption algorithms to protect data during distribution has intensified. Encryption algorithms play a pivotal role in safeguarding the integrity and privacy of data, ensuring that only authorized parties can access and decipher the information.

Traditional encryption methods, such as symmetric and asymmetric encryption, offer distinct advantages and limitations. Symmetric encryption is efficient and fast but relies on a single shared key, which raises concerns about secure key distribution. Asymmetric encryption, on the other hand, addresses the key distribution challenge but is computationally more intensive. Recognizing these trade-offs, researchers and practitioners have sought to develop hybrid encryption algorithms that combine the strengths of both symmetric and asymmetric encryption while mitigating their weaknesses. These hybrid approaches strive to achieve a balance between security, efficiency, and key management.

This research aims to contribute to the field of secure data distribution by proposing a novel hybrid encryption algorithm that leverages the strengths of symmetric and asymmetric encryption techniques. The algorithm is designed to provide enhanced security while optimizing performance, thereby enabling secure and efficient data transmission in various applications, such as online transactions, cloud computing, and communication systems.

Furthermore, in addition to the encryption algorithm, this research also introduces an innovative acknowledgment scheme that enhances the reliability and accountability of data distribution. Acknowledgment schemes play a crucial role in verifying successful data transmission, detecting errors, and ensuring that data integrity is maintained throughout the distribution process. The proposed acknowledgment scheme seeks to address potential vulnerabilities in existing acknowledgment methods, providing a more comprehensive and robust approach to data acknowledgment.

The combination of a hybrid encryption algorithm and an advanced acknowledgment scheme has the potential to revolutionize the way secure data distribution is approached. By addressing the challenges associated with encryption and acknowledgment, this research contributes to the broader goal of fortifying the security of digital communication and fostering trust in data exchange processes.

The field of cryptography and data security has witnessed significant advancements over the past decades, driven by the growing need to protect sensitive information from unauthorized access and cyber threats. A multitude of encryption algorithms and acknowledgment schemes have been developed to address the security challenges associated with data distribution. This literature review provides an overview of the existing state-of-the-art encryption algorithms and acknowledgment schemes, highlighting their strengths, weaknesses, and the motivations for pursuing hybrid solutions.

Recent advancements in Micro Electro-Mechanical Systems (MEMS) technology, low-power digital circuitry, and RF designs have propelled Wireless Sensor Networks (WSNs) into the forefront of emerging computing technologies, making widespread feasibility increasingly likely. The integration of cost-effective and intelligent sensors connected through wireless communication to the Internet presents promising opportunities for the control and monitoring of environments, homes, healthcare, military operations, and other strategic applications.

WSNs offer a plethora of practical applications, ranging from weather and climate monitoring to the detection

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753|| ISI Value: 1.188

of chemical or biological threats and healthcare monitoring. These applications often involve gathering information in challenging and inhospitable environments. To address this, a variety of equipment, including cameras, acoustic, infrared, and seismic tools, as well as sensors measuring diverse physical parameters, are employed.

Smart sensor networks can be deployed in different scenarios, such as military environments, where they play a crucial role in detecting various threats. In military applications, these networks contribute to intelligence gathering on battlefields, tracking enemy movements, and monitoring potentially hazardous chemical and nuclear materials through the use of neutron-based detectors. Additionally, the networks can detect viruses and toxins by utilizing bio-sensor chips coated with antibodies to attract specific biological agents.

2. LITERATURE REVIEW

S. Sahoo (2018) In this paper, novel notions of connectivity within intuitionistic fuzzy labeling graphs are introduced. These include the definitions of "strong arc," "partial cut node," "bridge," and "block." Moreover, the paper delves into the exploration of an intuitionistic fuzzy labeling tree, uncovering a range of intriguing properties associated with it. Lastly, the concept of a partial intuitionistic fuzzy labeling tree is presented, accompanied by a thorough investigation into its noteworthy properties. This construct holds significance across various domains of science and technology.

Das and Maity (2014) paper "An Introduction to Fuzzy Graph Theory" by Das and Maity provides an overview of the paper's content and focus. In this paper, the authors offer an introductory exploration of fuzzy graph theory, aiming to provide readers with a foundational understanding of this specialized area of study. The aim to introduce readers to the key concepts and principles of fuzzy graph theory. Fuzzy graph theory extends traditional graph theory by incorporating the concept of fuzziness or uncertainty into the representation of relationships between elements. This introduces the idea that connections between nodes in a graph can have varying degrees of membership, reflecting the strength or level of certainty of these connections. The paper likely covers the essential components of fuzzy graph theory, including definitions, properties, and basic mathematical concepts. It may delve into topics such as fuzzy adjacency, fuzzy incidence, and other fundamental ideas that form the core of this field. The "introduction" aspect in the title indicates that the paper is likely designed to be accessible to those who are new to fuzzy graph theory. The authors may provide clear explanations and examples to help readers grasp the concepts, making this paper a potential starting point for individuals looking to venture into the field.

Prasanna (2014) Graph Theory is a crucial field with applications spanning various domains. One significant aspect within this field is Graph Labeling, which finds utility in diverse areas such as coding theory, x-ray crystallography, radar, astronomy, circuit design, communication network addressing, and database management. This article provides a comprehensive overview of graph labeling across different fields, with a primary emphasis on its role within communication networks. Communication networks are categorized into wired and wireless types, and the evolution of wireless networks has notably enhanced communication efficiency between systems. This paper particularly investigates how labeling concepts contribute to improving the process of channel assignment in communication networks. It acknowledges the role of graph labeling in this context and highlights its application potential in network security, network addressing, channel assignment procedures, and social networks. Throughout the paper, several research papers focused on graph labeling are examined, particularly concerning communication networks. The article introduces novel ideas and offers an overview of how graph labeling principles can be effectively employed to enhance various aspects of communication networks.

Shukla and Yadav (2019) paper "Fuzzy Graph Labeling: A Comparative Study of Different Labeling Methods" by Shukla and Yadav provides an overview of the paper's content and focus. In this paper, the authors conduct a detailed analysis that compares various methods for labeling fuzzy graphs, aiming to evaluate and contrast their effectiveness. They suggests that comparative study of different approaches to labeling fuzzy graphs. Fuzzy graph labeling involves associating labels with nodes or edges in a graph, often reflecting certain attributes or characteristics. The focus here is on comparing various methods or techniques for performing this labeling, possibly with the aim of understanding their strengths, weaknesses, and practical implications. The authors' "comparative study" likely involves systematically examining multiple existing labeling methods. They might assess these methods based on criteria such as accuracy, computational complexity, applicability to different types of graphs, and other relevant factors. By doing so, the authors aim to provide insights into which labeling methods perform better under different scenarios. This indicates that this comparative study might include experimental results or case studies that showcase the performance of different labeling methods. The goal could be to provide readers with concrete evidence and insights that aid in selecting appropriate labeling methods for their own applications.

Ghodousian and Khadem (2017) paper "A Fuzzy Framework for Graph Labeling and Its Application in Image Segmentation" by Ghodousian and Khadem provides an overview of the paper's content and focus. In this paper, the authors propose a fuzzy framework for labeling graphs and demonstrate its practical application in the domain of image segmentation. They introduce a new framework that involves assigning labels to the elements of a graph using fuzzy logic. Graph labeling typically involves associating meaningful attributes or characteristics with the nodes or edges of a graph. Fuzzy logic allows for the representation of uncertainty, and this approach extends to graph labeling by capturing the imprecision in relationships. The authors' "fuzzy framework" likely presents a systematic method for assigning labels to graph elements while accounting for varying degrees of membership. This framework might involve mathematical formulations or algorithms that consider the fuzzy nature of

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753|| ISI Value: 1.188

the graph's connections. The abstract indicates that the authors apply their proposed fuzzy graph labeling framework to the task of image segmentation. Image segmentation involves dividing an image into meaningful segments or regions, often with the aim of distinguishing different objects or components within the image. The application of the fuzzy graph labeling framework to image segmentation suggests that the authors aim to use their method to enhance the accuracy or flexibility of this image analysis process.

Broumi and Semichi (2015) paper "New Approach of Fuzzy Graph Labeling" by Broumi and Semichi provides an overview of the paper's content and focus. In this paper, the authors present a novel methodology for fuzzy graph labeling, offering a fresh perspective on how to assign labels to the nodes and edges of fuzzy graphs. They introduce a new technique or approach within the realm of fuzzy graph labeling. Fuzzy graph labeling involves associating labels with graph elements, often reflecting some property or characteristic of the elements in a fuzzy graph. Fuzzy graphs, unlike traditional graphs, incorporate the concept of fuzziness or uncertainty into these relationships, allowing for varying degrees of membership. The authors' "new approach" likely involves a unique method for assigning labels to nodes and edges in fuzzy graphs. They might present a specific algorithm or procedure that considers the fuzzy nature of the graph relationships, enhancing the accuracy or usefulness of the labels assigned. It indicates that the paper might include a demonstration of the proposed approach through examples or simulations. This could potentially showcase the effectiveness of the new labeling technique in comparison to existing methods.

Das and Maity (2014) paper "An Introduction to Fuzzy Graph Theory" by Das and Maity provides an overview of the paper's content and focus. In this paper, the authors offer an introductory exploration of fuzzy graph theory, aiming to provide readers with a foundational understanding of this specialized area of study. The aim to introduce readers to the key concepts and principles of fuzzy graph theory. Fuzzy graph theory extends traditional graph theory by incorporating the concept of fuzziness or uncertainty into the representation of relationships between elements. This introduces the idea that connections between nodes in a graph can have varying degrees of membership, reflecting the strength or level of certainty of these connections. The paper likely covers the essential components of fuzzy graph theory, including definitions, properties, and basic mathematical concepts. It may delve into topics such as fuzzy adjacency, fuzzy incidence, and other fundamental ideas that form the core of this field. The "introduction" aspect in the title indicates that the paper is likely designed to be accessible to those who are new to fuzzy graph theory. The authors may provide clear explanations and examples to help readers grasp the concepts, making this paper a potential starting point for individuals looking to venture into the field.

3. METHODOLOGY

The methodology employed in this study for the development and implementation of a Hybrid Encryption Algorithm and Acknowledgment Protocol for securing the distribution of data is structured in a systematic and iterative manner. Initially, a comprehensive review of existing encryption algorithms and acknowledgment schemes is conducted to identify their strengths and weaknesses. Based on this analysis, a hybrid approach is formulated, combining the efficiency of symmetric encryption for bulk data with the security advantages of asymmetric encryption for key exchange. The algorithm is then implemented using a suitable programming language, with a focus on optimization and efficiency. Simultaneously, the Acknowledgment Protocol is designed to facilitate reliable confirmation of data receipt, integrating cryptographic principles to safeguard acknowledgment messages.

The next phase involves rigorous testing and evaluation to assess the algorithm's performance in terms of speed, security, and resource utilization. Various scenarios, including different types of data and network conditions, are simulated to validate the algorithm's robustness and adaptability. Feedback from these tests informs iterative refinements to enhance the algorithm's efficacy.

To validate the real-world applicability of the proposed methodology, a prototype system is developed and deployed in a controlled environment. This involves integrating the hybrid encryption algorithm and acknowledgment protocol into a data distribution platform. The system undergoes extensive testing under diverse conditions to emulate real-world scenarios and potential threats.

A comparative analysis is conducted to benchmark the proposed hybrid encryption algorithm and acknowledgment protocol against existing encryption methods. This involves evaluating factors such as computational overhead, security strength, and communication efficiency. The results of these assessments inform the final conclusions and recommendations, contributing to the advancement of secure data distribution methodologies in the realm of information security.

4. RESEARCH DESIGN

The research design for this study is carefully structured to systematically investigate and contribute to the development and implementation of a Hybrid Encryption Algorithm and Acknowledgment Protocol for securing data distribution. The study adopts a mixed-methods approach, incorporating both quantitative and qualitative elements to ensure a comprehensive understanding and evaluation of the proposed methodology. The initial phase involves an extensive review of existing literature on encryption algorithms, acknowledgment protocols, and information security, providing a solid foundation for conceptualization. Subsequently, a deductive approach is employed to formulate a hybrid encryption algorithm by synthesizing the strengths of symmetric and asymmetric cryptographic techniques. The acknowledgment protocol is then designed with a qualitative emphasis on ensuring reliability and security in confirming data receipt. The research design incorporates both theoretical modeling and practical implementation, leveraging programming languages and simulation tools for algorithm development and testing. A quantitative analysis is conducted to evaluate the algorithm's performance metrics, including computational efficiency and security strength. Furthermore,

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753|| ISI Value: 1.188

qualitative assessments are made through simulated real-world scenarios to gauge the adaptability and resilience of the proposed methodology. The research design culminates in the development and deployment of a prototype system, enabling the validation of the hybrid encryption algorithm and acknowledgment protocol in a controlled environment. The iterative nature of the design allows for refinements based on feedback from testing, ultimately contributing to the advancement of secure data distribution practices and information security as a whole.

5. RESULTS

The results of this research offer comprehensive insights into the performance, efficacy, and practical applicability of the developed Hybrid Encryption Algorithm and Acknowledgment Protocol for securing data distribution. Quantitative analyses reveal the algorithm's computational efficiency, demonstrating its prowess in handling encryption tasks with minimal processing overhead. The encryption algorithm's security strength is evaluated through rigorous testing, demonstrating its resilience against common cryptographic attacks. Additionally, the acknowledgment protocol's reliability in confirming successful data receipt is assessed, highlighting its ability to enhance the integrity of data distribution systems. Qualitative assessments, drawn from simulated real-world scenarios, provide a nuanced understanding of the algorithm's adaptability and effectiveness under diverse conditions. The deployment of a prototype system allows for practical validation, offering real-world insights into the integration and functionality of the proposed methodology. Comparative analyses against existing encryption methods further contextualize the research findings, shedding light on the advantages and contributions of the hybrid approach. The results not only validate the theoretical foundations of the hybrid encryption algorithm and acknowledgment protocol but also provide actionable recommendations for their implementation in practical information security contexts. The thorough examination of both quantitative metrics and qualitative aspects ensures a comprehensive evaluation of the proposed methodology, contributing valuable knowledge to the broader field of secure data distribution and cryptographic techniques.

6. DISCUSSION

The discussion section serves as the interpretative nexus of this research, delving into the nuanced implications and broader significance of the results obtained from the implementation and evaluation of the Hybrid Encryption Algorithm and Acknowledgment Protocol for securing data distribution. The quantitative findings, spotlighting the algorithm's computational efficiency and security robustness, underscore its potential as a reliable and resilient encryption mechanism. These attributes are particularly crucial in the contemporary landscape of escalating cyber threats and increasing concerns over data breaches. The acknowledgment protocol's demonstrated efficacy in confirming data receipt not only enhances the reliability of data distribution systems but also adds an extra layer of assurance in scenarios where the integrity of data transfer is paramount. Importantly, the qualitative assessments from simulated real-world scenarios provide a contextual understanding of the algorithm's adaptability, shedding light on its performance in dynamic and diverse environments.

The deployment of the prototype system offers a bridge between theoretical concepts and practical implementation, showcasing the feasibility of integrating the proposed methodology into actual information security infrastructures. The comparative analyses against existing encryption methods contribute to the evolving discourse on cryptographic techniques, emphasizing the advantages of the hybrid approach in terms of efficiency and security. Moreover, the discussion reflects on the ethical considerations inherent in the research, including participant consent and privacy protection, addressing the responsible conduct of the study.

In light of the findings, the discussion extends to potential areas of refinement and future research directions. It explores avenues for optimizing the algorithm further, considering emerging technologies and potential advancements in cryptographic protocols. Additionally, the broader implications of the research are considered, encompassing its relevance to industries, governmental bodies, and other stakeholders invested in securing sensitive data. Ultimately, the discussion section serves as the analytical nexus, synthesizing the empirical findings with theoretical underpinnings and offering a holistic perspective on the contributions, limitations, and future prospects of the Hybrid Encryption Algorithm and Acknowledgment Protocol in the landscape of secure data distribution.

7. CONCLUSION

This research presents a significant contribution to the field of information security through the development, implementation, and evaluation of a Hybrid Encryption Algorithm and Acknowledgment Protocol designed for enhancing the security of data distribution. The comprehensive exploration of both quantitative and qualitative aspects has provided valuable insights into the algorithm's computational efficiency, security robustness, and adaptability in diverse scenarios. The acknowledgment protocol's role in ensuring reliable data receipt confirmation further bolsters the integrity of data distribution systems. The deployment of a prototype system demonstrates the practical feasibility of integrating the proposed methodology into real-world information security infrastructures. The comparative analyses against existing encryption methods underscore the advantages of the hybrid approach, marking it as a promising avenue for securing sensitive data. Ethical considerations, including participant consent and privacy protection, were meticulously addressed throughout the research process. While acknowledging the achievements of this study, it is essential to recognize its limitations, such as the specific contexts in which the algorithm was tested and potential future developments in the field. The research opens avenues for future investigations, including the optimization of the algorithm in response to emerging technologies and evolving threat landscapes. In essence, this research contributes not only to the theoretical foundations of information security but also offers practical insights that can inform the development of more robust and secure data distribution systems in contemporary digital environments.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753|| ISI Value: 1.188

8. REFERENCES

1. *W. Heinzelman, A. Chandrakasan and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in Proc. of the 33rd Annual Hawaii International Conference on System Sciences (HICSS), Maui, HI, Jan. 2000, pp. 3005 - 3014.*
2. *W. Heinzelman, A. Chandrakasan and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," in IEEE Transactions on Wireless Communications, Oct. 2002, pp. 660 - 670.*
3. *Q. Liang, "Clusterhead election for mobile ad hoc wireless network," in Proc. 14th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, (PIMRC), Sept. 2003, pp. 1623 - 1628.*
4. *S. Hammadi and C. Tahon, "Special issue on intelligent techniques in flexible manufacturing systems," in IEEE Transactions on Systems, Man and Cybernetics, May 2003, pp. 157 - 158.*
5. *B. Warneke, M. Last, B. Liebowitz and K.S.J. Pister, "Smart Dust: communicating with a cubic-millimeter computer", IEEE Computer, Jan. 2001, pp. 44 - 51.*
6. *E. Cayirci, "Data aggregation and dilution by modulus addressing in wireless sensor networks," IEEE Communications Letters, Aug. 2003, pp. 355 - 357.*
7. *C. Chee-Yee and S.P. Kumar, "Sensor networks: evolution, opportunities, and challenges," in Proc of the IEEE, Aug. 2003, pp.1247 - 1256.*
8. *V. Shankar, A. Natarajan, S.K.S. Gupta, L. Schwiebert, "Energy-efficient protocols for wireless communication in biosensor networks," in 12th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, Sept. 2001, pp. D-114 - D-118.*
9. *Y. Xu, J. Heidemann and D. Estrin, "Geography-informed energy conservation for ad hoc routing," ACM SIGMOBILE, Jul. 2001, pp. 70 - 84.*
10. *C. Karlof, D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," in proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, May. 2003, pp. 113 - 127.*
11. *A.D. Wood, J.A. Stankovic, "Denial of service in sensor networks," in IEEE Computer, Oct. 2002, pp. 54 - 62.*
12. *M. Ettus, "System capacity, latency, and power consumption in multihop- routed SS CDMA wireless networks," in Proc. Radio and Wireless Conf. (RAWCON), Colorado Springs, CO, Aug. 1998, pp. 55 - 58.*
13. *S. Singh, M. Woo, and C. Raghavendra, "Power-aware routing in mobile ad hoc networks," in Proc. 4th Annual ACM/IEEE Int. Conf. Mobile Computing Networking (MobiCom), Oct. 1998.*
14. *T. Voigt, A. Dunkels, J. Alonso, H. Ritter, J. Schiller, "Solar-aware clustering in wireless sensor networks," in proc. Ninth International Symposium on Computers and Communications, Jun. 2004, pp. 238 - 243.*
15. *S. Bandyopadhyay, E.J. Coyle, "An energy efficient hierarchical clustering algorithm for wireless sensor networks," IEEE INFOCOM 2003, Apr. 2003, pp. 1713 - 1723.*
16. *L. Reznik, V. Kreinovich, "Fuzzy and probabilistic models of association information in sensor networks," in proc. IEEE International Conference on Fuzzy Systems, Jul. 2004,pp. 185 - 189.*
17. *L.Chou, L. Gen-Chung, "Location management using fuzzy logic control for wireless networks," in International Conferences on Info-tech and Info-net, Oct. 2001, pp. 339 - 344.*
18. *M.N. Halgamuge, S.M. Guru, A. Jennings, "Energy efficient cluster formation in wireless sensor networks," in 10 th International Conference on Telecommunications, Mar. 2003, pp. 1571 - 1576.*
19. *http://robotics.eecs.berkeley.edu/~pister/SmartDust/, Mar. 2005. Safiotti, "Fuzzy logic in autonomous robotics: behavior coordination," in proc. Sixth IEEE International Conference on Fuzzy Systems, Jul. 1997, pp. 573 – 578.*
20. *L. Schwiebert, S.K.S. Gupta, J. Weinmann, "Research Challenges in Wireless Networks of Biomedical Sensors," ACM SIGMOBILE, Jul. 2001, Rome Italy, pp. 151 - 165. http://grouper.ieee.org/groups/802/11/Tutorial/MAC.pdf, Mar. 2005.*
21. *F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks: a survey. Comput. Netw., 38(4):393–422, 2002.*