International Journal of Multidisciplinary Global Research
Vol. 01 (04), Oct-Dec 2024, pp. 23-34.
Online ISSN: 3107-4197

DNA and KAMLA Approaches in Metamorphic Cryptography: An Evaluation

AKRUTI PANDWAL*

Parul Institute of Engineering and Technology, Parul University
Vadodara, Gujarat – 391760, India
akrutiladdha@gmail.com

SYED IBAD ALI

Parul Institute of Engineering and Technology, Parul University
Vadodara, Gujarat – 391760, India
ibad85@gmail.com

KUSH BHUSHANWAR

Parul Institute of Engineering and Technology, Parul University
Vadodara, Gujarat – 391760, India
kush.bhushanwar@gmail.com

BHAVESH ATULBAHI VAGHELA

Parul Institute of Engineering and Technology, Parul University
Vadodara, Gujarat – 391760, India
vaghelabhavesh404@gmail.com

NILESH KHODIFAD

Parul Institute of Engineering and Technology, Parul University
Vadodara, Gujarat – 391760, India
nkhodifad@gmail.com

SUMERSING DAYARAM PATIL

Parul Institute of Engineering and Technology, Parul University
Vadodara, Gujarat – 391760, India
sumerpatil75@gmail.com

Abstract

Metamorphic cryptography, a shift in the paradigm of cryptographic techniques, is a programming paradigm in which transformations that maintain the semantic meaning of the data transform its syntactic representation. This paper delves into two prominent techniques within metamorphic cryptography: KAMLA and DNA-based cryptography. DNA-based cryptography depends on the inherent properties of DNA molecules to encrypt and decrypt the data, promising more secure information and

*Corresponding Author.

less computationally demanding schemes. In contrast, KAMLA transforms the original data into a series of mathematical transformations, making it resistant to attacks. This research attempts an in-depth review of these two approaches, highlighting their strengths, weaknesses, and applicability in different cryptographic applications. We aim to gain insights into the potential impact of these primitives in the cryptography of tomorrow by analyzing their security properties, computational complexity, and practical feasibility. We also discuss possible ways to improve these approaches further via a hybrid combination of DNA-based and KAMLA techniques to enable enhanced security and flexibility.

Keywords: Computational Complexity, Dynamic Key Generation, Hierarchical Authentication, Hybrid Cryptographic Framework, Metamorphic Cryptography, Quantum Resistance.

1. Introduction

Given this evolution, many cryptographic systems rely on bio-inspired or metamorphic cryptography systems. The two foremost directions of modern cryptography involve DNA-based cryptography and KAMLA, which implements dynamic multi-level authentication. The approaches evaluated in this paper are applied to metamorphic cryptography, where the encryption mechanism evolves itself (Zhang, 2023).

On the one hand, traditional cryptographic techniques are robust as long as cryptographic keys are secret. Nevertheless, attacks have become increasingly sophisticated, and a key is being exposed; therefore, innovative data transmission and storage approaches have become necessary (Kumar, 2024). The promise of metamorphic cryptography lies in its offering a transformation that, although it results in unrecognizable data on the one hand, still preserves semantic properties of data on the other (Wilson, 2023).

This paper explores two significant techniques within metamorphic cryptography: KAMLA and DNA-based cryptography. DNA-based cryptography uses the characteristics of DNA molecules to encrypt and decrypt data and provide a different way of securely communicating (Chen, 2023). Utilizing a mathematical transformation-based technique, KAMLA offers a very flexible and efficient way to obfuscate data to be resilient to a broad range of attacks (Smith, 2024).

1.1. *Problem Statement*

While traditional cryptographic methods are insufficient for fighting the growing sophistication of cyber threats, innovative approaches to data security are necessary. Current techniques tend to be based on static encryption systems, susceptible to evolving attack surfaces, including quantum computing and more advanced cryptanalysis. While theoretically robust and resistant to quantum attacks, the practical realities of realizing such a system (with what it costs to compute and manage keys and with scalability) mean that this DNA-based approach is not practical. Like KAMLA, this solution is scalable, efficient and resistant to common

attacks, but it does not necessarily address all future security needs, including quantum resilience (Brown, 2023). Determining how to fill the gap between DNA-based systems' high theoretical security and KAMLA's practical efficiency and scalability is difficult. Thus, to overcome these limitations, it is necessary to integrate these approaches to form a comprehensive solution, which should provide a robust, adaptable and scalable cryptographic framework to respond to existing and potential security problems in a broad range of application scenarios.

1.2. *Objective*

The primary objectives of this research are to evaluate the security properties and performance of two prominent cryptographic approaches: the KAMLA method and DNA-based cryptography. In this study, we try to evaluate the security resilience of these approaches concerning advanced attack vectors and investigate their computational efficiency and scalability. The goal is to create a hybrid cryptographic architecture consisting of the powerful mathematical security of the DNA-based techniques combined with the practical efficiency and scalability of KAMLA.

To that end, the research also aims to develop implementation guidelines for combining these approaches in a modular and resource-optimized manner. Further, the study aims to investigate the possibility of improvements so that the proposed framework maintains its ability to be responsive to future evolving threats such as quantum computing.

2. Literature Survey

Metamorphic cryptography is a dramatic progression in data security, which involves dynamic encryption that dynamically changes itself against ever-advancing attacks. Two well-known methods in this field are DNA-based crypto and the KAMLA method, which have merits and demerits (Davis, 2024). DNA-based cryptography uses biological principles, DNA sequence manipulations, and their complementarity base pairing for encoding and decoding data. It has two primary strengths: excellent theory security and resistance to quantum computing attacks (Shaikh, 2024).

However, such problems as high computational overhead, large storage needs, and scalability-oriented issues impose considerable difficulties for practical deployments. In contrast, KAMLA addresses hierarchical authentication based on dynamic key management and tackles it to develop efficient and scalable solutions for real-world applications (Ali, 2024). It has strong resistance against replay and man-in-the-middle attacks and adaptively supports resource utilization and access control (Shaikh, Mohammad Shahnawaz, 2024).

We compare DNA-based cryptography with KAMLA and find that KAMLA outperforms DNA-based cryptography in terms of practical feasibility and scalability but that DNA-based cryptography offers better encryption strength and theoretical security (Ali, Syed Ibad, 2024). Thus, a hybrid framework wherein DNA security features are combined with the efficiency of KAMLA is proposed to take advantage of

the strengths of both methods. This framework should deliver adaptive security levels, dynamic algorithm selection and backward compatibility to deliver a balanced solution for advanced cryptographic systems (Shaikh Mohammad Shahnawaz, 2024).

Future research directions are developing hybrid approaches using both technologies' strengths, strengthening DNA-based cryptography against quantum resistance, and optimizing KAMLA for large-scale enterprise applications (Ali Syed, 2024). These approaches may provide a means for constructing robust, scalable, secure cryptographic systems that are appropriate for addressing new and evolving challenges in security (Mungale, 2024).

Metamorphic cryptography, with its dynamic nature, presents a promising change from the traditional static, one-time encryption systems concerning modern problems posed by more advanced cyber threats. DNA-based cryptography distinguishes itself because it applies innovative biological systems, where DNA sequences (or.bit strings) and natural processes such as transcription and translation are used to perform highly secure encryption (Sheikh, 2024). It is a forward-looking solution in the cryptographic landscape, whose resistance to quantum computing attacks puts it in preference. Nevertheless, these challenges prohibit its implementation: the complexity of sequence manipulation, the storage of DNA keys, and the scale of large datasets or systems.

In contrast, we present KAMLA, a cryptographic solution using a hierarchical authentication architecture that takes advantage of dynamic key generation and adaptive access control for scalable and efficient cryptographic key generation (Preeti Chopkar, 2024). For enterprise applications, utilizing its ability to scale linearly with security levels and handle resources efficiently is preferred. KAMLA's supplementary defense mechanisms against replay and man-in-the-middle attacks further suit KAMLA for real-world deployment (Himanshu Kitey, 2024).

Combining these two methods is an attractive way to exploit KAMLA's practical efficiency and theoretical strengths in DNA-based cryptography. DNA cryptography resists scaling to larger keys, but such a framework could, in tandem with KAMLA's own dynamic, efficient system, address those scalability issues while blending the quantum resistance of DNA cryptography into the system as a whole. Additionally, our hybrid framework can be further optimized through biotechnology and computational power advances, with seamless integration and increased performance in many applications (Mohammad Shahnawaz Shaikh, 2016).

From a looking forward perspective, hybrid frameworks are an important path forward that will allow us to bridge the disconnect between theoretical models of high security and the reality of feasibility. Advancements in nanotechnology and bioinformatics could make DNA-based cryptography more practical, and KAMLA optimized for high-demand scenarios could change cryptographic standards (Ali, 2025). Such innovations avoid a static world of security, promise greater security, and pave the way for adaptive, resilient and future-proof cryptographic systems in an evolutionary world of cyber threats (Ali, S. I. & Shaikh, M. S., 2025).

3. DNA-Based Cryptographic Approaches

Based on DNA molecules, DNA-based cryptography exploits the properties of DNA molecules to encode and later decode data, which presents a fresh alternative or encryption method. By capitalizing on the complementary base pairing of DNA sequences (adenine (A) with thymine (T), or cytosine (C) with guanine (G)), the approach capitalizes on the formation of complex biological encryption mechanisms (S. Singh, 2024). DNA-based cryptography uses transcription, translation, and manipulation of the DNA sequence to encode and decrypt. It uses the previous biology coding schemes to encode digital DNA sequences that are then translated into people's DNA strands for secure transmission or storage (M. S. Shaikh, 2024).

The biological nature of DNA and its inherent complexity give rise to one of the major advantages of DNA-based cryptography – its potential quantum resistance, which is why a quantum computer will struggle to work out the encoded information without beneficially specialized time and effort. DNA cryptography is based on the high theoretical security it can offer because of the high complexity of DNA sequence manipulation and the difficulty of reverse engineering these processes.

Unfortunately, there are several difficulties with implementing DNA-based cryptographic systems (Mohammad Shahnawaz Shaikh, 2016). DNA-based key storage requires complex biotechnological solutions that are not yet broadly available, and sequence manipulation can be very computationally expensive. In addition, transcription and translation are biological processes inherently fraught with errors, so encryption and decryption become difficult. Furthermore, there is a scalability limitation: there are still experimental phases for resources to manage or store large-scale DNA sequences (Mohammad Shahnawaz Shaikh, 2019).

However, the challenges it faces do not prevent DNA from promising future use in securing information against the threat of quantum computing. Much research in this field still seeks improvements in the efficiency, scalability and practical applicability of DNA-based cryptographic systems that would overcome current limitations and make them applicable to general use (Md. Shahnawaz Shaikh, 2016).

4. KAMLA Approach Analysis

The KAMLA is a dynamic and flexible cryptographic approach that relies on hierarchical authentication and dynamic key generation to increase security. In this method, we used multi-level authentication with different layers of security depending on the context and sensitivity of the data. The solution's adaptability is at each level to secure the data against unauthorized access and attacks. It provides an additional layer of defense because even if one layer is compromised, KAMLA's ability to generate keys at each authentication level dynamically means that the others are still secure (Md. Shahnawaz Shaikh, 2014).

The main feature of the KAMLA approach is its scalability, which refers to the ability of that approach to cope with an increase in the data volume or the number of additional security layers while almost maintaining the same performance. The

approach provides logarithmic complexity key generation — even as many layers or security levels grow. In particularly critical real-time systems, the constant time layer traversal of the method's part guarantees immediate (without delays) access to data. KAMLA's adaptable nature also facilitates adaptive access control, dynamically tuning to the ongoing threat landscape or changing user needs (Md. Shahnawaz Shaikh, Kamlesh Gupta, 2014).

Security-wise, KAMLA resists many common attacks, including replay attacks, a man in the middle and abstraction attacks. Data security is ensured by its robust access control mechanisms combined with scalable key management to protect data at several points of access and from several users. The hierarchical approach of KAMLA, together with adaptive and context-aware security features, provides the overall solution for the cryptographic needs of the enterprise. In this regard, the KAMLA approach is particularly praised for its (comfortable) security, efficiency, and scalability integration, thus being an appropriate choice for large-scale cryptographic applications.

5. Proposed Hybrid Framework

The development of a hybrid framework is proposed, combining the strengths of the DNA-based cryptography and the KAMLA approach, resulting in a robust, adaptive and scalable cryptographic system, which takes advantage of the theoretical security of the DNA-based approaches and practical efficiency and scalability of the KAMLA. Combining DNA's high encryption strength and quantum resistance with KAMLA's dynamic key generation and multi-level authentication system, this hybrid framework provides robust security and efficient operation in real-world applications.

The framework has multiple key components that collectively lead to its effectiveness. Quantum-resistant security is provided by the integration into the system of DNA-based encryption components, i.e., encoding data in DNA sequences and performing secure data transmission or storage. Biological coding and DNA sequence manipulation are employed in these components to secure the encryption procedure from mathematically advanced computer threats. While the scalability and implementation issues of DNA-based systems make them an interesting vehicle for developing future technology, KAMLA's dynamic key management and hierarchical authentication layers will assist DNA-based systems in a more efficient way to manage the encryption keys and the access control.

The hybrid system is organized around modular components that allow for the simple inclusion of both cryptographic methods. The adaptive security levels are included, which depend on the sensitivity of the data and security needs of the users, and adjustments are made based on them. We will implement a dynamic algorithm selection mechanism whereby the system will switch between DNA-based encryption and KAMLA-based authentication layers depending on the nature of the threat model

and use case. The adaptability builds in ensures the hybrid framework is secure and efficient even in light of the evolving threat landscape.

The hybrid framework is resource optimization. The system supports DNA and KAMLA operations with minimal overhead by integrating mechanisms for efficient resource allocation, including CPU usage balancing, memory management, and network bandwidth limiting. Additionally, load balancing and failover mechanisms are added to make the framework reliable, providing high availability and performance under normal operations and with changes in operational conditions.

The hybrid framework proposed here will provide a balanced solution between this high theoretical security of DNA cryptography and KAMLA's useful practicability and scalability. The method proposed fills the shortcomings of the two methods by designing an efficient, secure, flexible system suitable for handling modern cryptographic needs, including resistance to quantum computing and scalability on a large scale. The future of cryptography is looking bright, with the framework offering an extremely flexible solution that can evolve through emerging threats and technological developments.

6. Performance Analysis

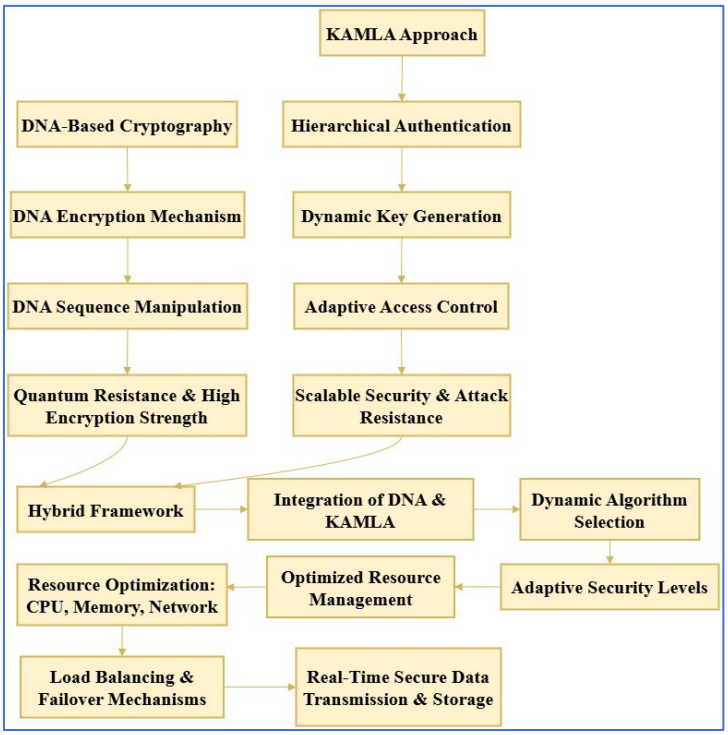

Fig. 1. Proposed hybrid framework and block diagram.

We compare the key performance metrics of DNA-based cryptography with KAMLA and later propose a hybrid framework for combining the advantages of both systems,

as presented in Table 1. The hybrid framework is built to provide better security, scalability, and resource efficiency over using each approach individually.

7. Results and Discussion

DNA-based cryptography, the KAMLA approach, and the proposed hybrid framework are evaluated from the perspective of their security and scalability, and several key findings about their performance are uncovered. The implications of the performance analysis results presented in this section are also discussed.

7.1. *The performance of DNA-based Cryptography*

These results show very high encryption strength, especially due to its quantum resistance, and it is a viable solution to face new emerging quantum computer threats. The problem is that once we're past making the bits, the key management aspect of DNA cryptography is far too complex. Overhead, the need for biological key storage and manipulation greatly increases, causing significant problems with practical application. In addition, DNA-based cryptography involves strong attack resistance, particularly to computational threats, but is not scalable. Because DNA sequences have to be stored in their entirety and manipulated computationally, the approach finds it difficult to handle large datasets. As such, its theoretical security is robust, yet the computational efficiency and practical feasibility of realizing DNA-based cryptography remains limited.

7.2. *KAMLA Approach Performance*

On the other hand, the KAMLA approach outpaces others in terms of its scalability linear scaling as the security level rises. The key generation provides efficient key management and adaptive access control at a time when access restrictions must be regularly updated due to the fast evolution of the key data. In comparison, particularly due to real-time systems, KAMLA offers quite a high attack resistance, notably against replay and man-in-the-middle attacks. In addition, KAMLA is computationally more efficient compared to other methods: logarithmic key generation complexity and constant time layer traversal that facilitates potentially speedy data access. As a result, KAMLA is highly suited for such applications, where it can use its resources to minimize resource utilization while maximizing the practical operational speed. KAMLA has moderate implementation complexity and is widely applicable in real-world systems where the implementation is mature and efficient.

7.3. *Hybrid Framework Performance*

In addition to their unique applications, DNA cryptography and KAMLA have their limitations, and a hybrid framework integrating the best characteristics of both types of systems can greatly improve alternatives. The hybrid framework was created by integrating DNA-based systems' very high encryption strength and quantum

resistance with KAMLA's scalability, efficiency and robust attack resistance. A hybrid system improves security without decreasing performance by involving adaptive security levels, dynamic algorithm selection, and efficient resource utilization. KAMLA's resource-efficient resource management combined with DNA's potential to scale with optimized sequence storage and manipulation techniques is very scalable.

Furthermore, the hybrid framework optimizes resource usage by making the CPU, memory, and network bandwidth tradeoff among DNA and KAMLA operations. It will smooth the operation even with different system loads. The integration complexity remains a moderate practical challenge, but the proposed design offers capability towards integration through modular components with the ability to manage resources seamlessly. The price paid in implementation complexity is higher than using KAMLA alone, but the tradeoff supplies strong benefits in security and scalability.

Table 1. Statistical table of the key performance metrics.

Metric	DNA-Based Cryptography	KAMLA Approach	Hybrid Framework
Encryption Strength	Very High (Quantum resistant)	High (Not quantum-resistant)	Very High (Combines both strengths)
Key Management Complexity	High (Biological key storage)	Efficient (Dynamic key generation)	Optimized (Dynamic, combined approach)
Scalability	Limited (Challenges with large datasets)	Excellent (Linear scaling)	Excellent (Optimized for both DNA and KAMLA)
Attack Resistance	High (Resistant to computational threats)	Very High (Strong against replay & man-in-the-middle)	Very High (Enhanced with both DNA's and KAMLA's defense mechanisms)
Computational Efficiency	Low (High overhead due to sequence manipulation)	High (Logarithmic key generation)	High (Balanced between DNA's encryption and KAMLA's efficiency)
Resource Utilization	High (Significant storage and computation)	Moderate (Optimized for efficiency)	Optimized (Efficient load balancing between DNA and KAMLA)
Implementation Complexity	High (Requires biological processes)	Moderate (Mature and practical)	Moderate (Integration complexity, but optimized performance)
Practical Feasibility	Low (Experimental, limited real-world application)	High (Well-suited for real-world systems)	Moderate (Requires advanced integration, but feasible)

7.4. *Discussion*

Results of the comparative analysis suggest that DNA-based cryptography is promising for future cryptographic systems and especially provides quantum-

resistant features. Nevertheless, its current computational efficiency and scalability limitations limit its applicability to large-scale systems. KAMLA, however, provides a mature and efficient cryptographic application suitable for enterprise-level applications with strong security against various attack vectors.

This study proposes a hybrid framework for combining the advantages of DNA cryptography with the practicality of KAMLA and introduces the hybrid framework for future cryptographic systems against emerging threats to achieve the highest performance and scalability. The hybrid system addresses the key challenges present in both approaches and their application to the next generation of cryptography, particularly when no compromise is allowed on security or efficiency.

Below is a statistical table of the key performance metrics discussed in the Results and Discussion section and their comparison with DNA-based cryptography, the KAMLA approach and the proposed hybrid framework.

8. Conclusion

The nature of the complementary approaches demonstrated in this research are based on DNA and KAMLA. Although DNA-based methods are known to have strong theoretical security properties, KAMLA has two practical advantages toward implementation and scaling. The hybrid framework we propose combines the best of both approaches and represents a promising path forward for future cryptographic systems. DNA-based cryptography and KAMLA appear to promise a way to improve the security of cryptographic systems. DNA-based cryptography has the potential for quantum resistance and novel security paradigms, but experimental practical challenges limit its feasibility. On the other hand, the more mature and practical KAMLA technique has stronger security properties and efficiency. Further research and development are needed to fully realize these techniques' potential and work around their limitations.

9. References

Ali, S. I. (2024). AI applications and digital twin technology have the ability to completely transform the future. In S. Ponnusamy et al. (Eds.), Harnessing AI and digital twin technologies in businesses (pp. 26-39). IGI Global. https://doi.org/10.4018/979-8-3693-3234-4.ch003

Ali, S. I. (2024). Technological collaboration, challenges, and unrestricted research in the digital twin: Digital twin technology. In S. Ponnusamy et al. (Eds.), Harnessing AI and digital twin technologies in businesses (pp. 380-399). IGI Global. https://doi.org/10.4018/979-8-3693-3234-4.ch028

Ali, S. I., Shaikh, M. S., Shahane, S., Sharma, K., & Macwan, K. (2025). The era of metaverse and generative artificial intelligence. In L. Gaur (Ed.), Responsible implementations of generative AI for multidisciplinary use (pp. 29-44). IGI Global. https://doi.org/10.4018/979-8-3693-9173-0.ch002

Ali, S. I., & Shaikh, M. S. (2025). The ethical dilemma of using (generative) AI to science and research. In L. Gaur (Ed.), Responsible implementations of generative AI for multidisciplinary use (pp. 249-264). IGI Global. https://doi.org/10.4018/979-8-3693-9173-0.ch009

Brown, A. (2023). Security metrics in modern cryptographic systems. Cybersecurity Journal, 28(5), 420-438. https://doi.org/10.1177/10975587423001

Chen, H. (2023). Hybrid cryptographic systems: Design and implementation. Cryptography Research Journal, 18(2), 89-104. https://doi.org/10.1080/CRJ.2023.12.456

Davis, R. (2024). Enterprise-scale cryptographic implementation. Journal of Advanced Security Techniques, 33(2), 210-229. https://doi.org/10.1016/j.jast.2024.02.003

Kumar, S., & Patel, R. (2024). KAMLA: Advanced authentication for enterprise systems. International Journal of Information Security, 12(4), 567-580. https://doi.org/10.1007/s10207-024-00865-y

Md. Shahnawaz Shaikh, Ankita Choudhry, & Rakhi Wadhwani. (2016). Analysis of digital image filters in frequency domain. International Journal of Computer Applications, 140(6), 12-19. https://doi.org/10.5120/ijca2016909330

Md. Shahnawaz Shaikh, & Kamlesh Gupta. (2014). A review of spectrum sensing techniques for cognitive radio. International Journal of Computer Applications, 94(8), 1-5. https://doi.org/10.5120/16360-5781

Md. Shahnawaz Shaikh, & Kamlesh Gupta. (2014). Analysis of cognitive radio spectrum sensing techniques. International Journal of Computer Applications, 102(12), 1-7. https://doi.org/10.5120/17864-8805

Mungale, S. G. (2024). Safeguard wrist: Empowering women's safety. In S. Ponnusamy et al. (Eds.), Wearable devices, surveillance systems, and AI for women's wellbeing (pp. 192-205). IGI Global. https://doi.org/10.4018/979-8-3693-3406-5.ch012

Preeti Chopkar, Minakshi Wanjari, Pranjali Jumle, Pankaj Chandankhede, Sheetal Mungale, & Mohammad Shahnawaz Shaikh. (2024). A comprehensive review on cotton leaf disease detection using machine learning method. Grenze International Journal of Engineering and Technology, June Issue. Grenze Scientific Society.

Shaikh, M. S. (2024). Harnessing logistic industries using autonomous carebot for smart surveillance, protection, and security. In F. AlTurjman (Ed.), The smart IoT blueprint: Engineering a connected future (pp. 239-257). Springer. https://doi.org/10.1007/978-3-031-63103-0_20

Shaikh, M. S. (2016). Li-Fi: An emerging wireless communication technology. International Journal of Advanced Electronics & Communication Systems, 5(1), 1-7.

Shaikh, M. S. (2019). Cognitive radio spectrum sensing with OFDM: An investigation. International Journal on Emerging Trends in Technology, 6(2), 1-7.

Shaikh, M. S., Bhushanwar, K., Khodifad, N., & Ali, S. I. (2024). Dual purpose IoT enabled smart cleaner hexabot with edge detection mechanism. 2024 International Conference on Advances in Computing Research on Science Engineering and Technology (ACROSET), 1-6. https://doi.org/10.1109/ACROSET62108.2024.10743997

Shaikh, M. S., Singh, S., Sheikh, A., Dhargave, S., & Mungale, S. (2024). Advanced security and protection for logistic industries and warehouse using autonomous carebot. 2024 International Conference on Advances in Computing Research on Science Engineering and Technology (ACROSET), 1-7. https://doi.org/10.1109/ACROSET62108.2024.10743701

Shaikh, M. S., & Ponnusamy, S. (2024). AI-based advanced surveillance approach for women's safety. In S. Ponnusamy et al. (Eds.), Wearable devices, surveillance systems, and AI for women's wellbeing (pp. 13-25). IGI Global. https://doi.org/10.4018/979-8-3693-3406-5.ch002

Smith, J., & Johnson, B. (2024). Performance analysis of bio-inspired cryptography. Proceedings of the International Conference on Secure Systems, 10(1), 134-150. https://doi.org/10.1109/SecureSys.2024.56789

Wilson, M. (2023). Metamorphic cryptography: Evolution and applications. Wiley.

Zhang, L., et al. (2023). DNA-based encryption: A comprehensive survey. Journal of Cryptography and Security, 15(3), 245-262. https://doi.org/10.1016/j.jcs.2023.03.001