Frontiers in Health Informatics ISSN-Online:2676-7104
www.healthinformaticsjournal.com
2024; Vol 13: Issue 3
Open Access

BEMSQIN: Design of an Efficient Hybrid Bioinspired Encryption Model for Enhancing Security of QoS-aware IoT Networks

[1] Dr .Dipalee Chaudhari, [2.] Dr.Kalyan Devappa Bamane, [3.] Dr.Shanthi Kumaraguru, [4.] Dr. Mane Vijay M, [5.] Dr. Abhijit Janardan Patankar, [6.] Mrs.Sulbha Yadav

[1]Assistant Professor, D.Y .Patil College of Engineering, Akurdi Pune-411044, ddrane@dypcoeakurdi.ac.in
[2]Associate Professor, D.Y .Patil College of Engineering, Akurdi Pune-411044, kdbamane@dypcoeakurdi.ac.in
[3]Assistant Professor, D.Y .Patil College of Engineering, Akurdi Pune-411044, skumarguru@dypcoeakurdi.ac.in
[4]Associate Professor, Department of Electronics and Telecommunications, Vishwakarma Institute of Technology, Pune, vijay.mane@vit.edu
[5]Associate Professor, D.Y .Patil College of Engineering, Akurdi Pune-411044, ajpatankar@dypcoeakurdi.ac.in
[6]Assistant Professor, Lokmanya Tilak College of Engineering koparkhairane, Navi Mumbai, sulbha.yadav@gmail.com, 400709

Cite this paper as: Dipalee Chaudhari,Kalyan Devappa Bamane, Shanthi Kumaraguru, Mane Vijay M, Abhijit Janardan Patankar, Sulbha Yadav (2024) BEMSQIN: Design of an Efficient Hybrid Bioinspired Encryption Model for Enhancing Security of QoS-aware IoT Networks. *Frontiers in Health Informatics, 13* (3), 8676-8692

Abstract

Strength and Quality-of-Service (QoS) performance of encryption techniques like Advanced Encryption Standard (AES), Elliptic Curve Cryptography (ECC), etc. depends upon their internal key configurations. Researchers have proposed a wide variety of models to optimize the security of these models while maintaining high QoS via dynamic programming techniques. But these techniques cannot be scaled for context-specific deployments, and cannot be reconfigured to support large-scale IoT (Internet of Things) Networks. To overcome these issues, this text proposes design of an efficient & Novel Elephant Herding Ant Lion Optimizer (EHALO), which assists in identification of security models & their internal configurations for different contextual deployments. The proposed model integrates spatial security performance with temporal communication performance in order to decide which encryption model to use, and then fuses this information with temporal security measures in order to identify optimal security configurations. These configurations are tested on multiple data level attack scenarios including Spoofing, Grey Hole, and Masquerading & Man-in-the-Middle (MITM) during identification of these configurations. Due to which the model is able to mitigate attacks with high efficiency while maintaining 8.3% lower delay, 4.5% higher energy efficiency, 9.5% higher throughput, and 2.4% higher packet delivery performance when compared with existing dynamic encryption models on similar attack scenarios.

Keywords: *Attack, Elephant Herding Algorithm, Ant colony optimization algorithm, QoS*

1. Introduction

Internet of Things (IoT) networks are becoming increasingly popular in various applications such as smart homes, healthcare, transportation, and agriculture. These networks consist of a large number of interconnected devices

that exchange sensitive data. However, the security of IoT networks is a major concern due to their distributed nature, resource constraints, and the increasing number of cyber-attacks which can be detected via chaotic non-orthogonal matrix (CNOM) [1, 2, 3].

One way to enhance the security of IoT networks is through encryption, which is a process of converting plain text data into an unreadable form to protect it from unauthorized access [4, 5, 6]. However, traditional encryption algorithms such as AES and RSA are not suitable for IoT networks due to their high computational complexity and energy consumption levels.

Bioinspired algorithms have been proposed as a promising approach to address the limitations of traditional encryption algorithms. These algorithms are inspired by the natural processes of biological systems, such as genetic algorithms, artificial neural networks, and ant colony optimization. They have shown promising results in various applications, including optimization, classification, and cryptography scenarios [7, 8, 9].

In this research paper, we propose a hybrid bioinspired encryption model that combines genetic algorithms, artificial neural networks, and chaos theory to enhance the security of Quality of Service (QoS)-aware IoT networks. The proposed model is designed to improve the encryption efficiency and reduce the computational complexity and energy consumption of traditional encryption algorithms.

The genetic algorithm is used to generate the initial population of encryption keys, which are optimized using the artificial neural network to improve the encryption quality. The chaos theory is used to enhance the randomness of the encryption keys and increase the resistance to attacks.

The performance of the proposed model is evaluated using various metrics, including encryption quality, computational complexity, energy consumption, and QoS. The results show that the proposed model outperforms traditional encryption algorithms in terms of security and efficiency levels.

The rest of the paper is organized as follows. Section 2 presents a literature review on bioinspired encryption algorithms and their applications in IoT networks. Section 3 describes the proposed hybrid bioinspired encryption model in detail. Section 4 presents the experimental setup and results; it also discusses the results and their implications. Finally, Section 5 concludes the paper and provides recommendations for future research scenarios.

2. Review of Existing Encryption Techniques

With the increasing popularity of IoT networks, the security of these networks has become a major concern. Encryption is an essential technique for securing IoT networks, but traditional encryption algorithms are not suitable for these networks due to their high computational complexity and energy consumption. Therefore, researchers have proposed various bioinspired encryption algorithms to address these limitations [10, 11, 12].

Genetic algorithms (GAs) are one of the bioinspired algorithms used in encryptions. GAs mimics the natural evolution process of biological systems and have been used to optimize the encryption keys. For example, in [13, 14, 15], a GA-based encryption scheme with Multikey homomorphic encryption (MKHE) was proposed for wireless sensor networks (WSNs) to enhance the security of these networks. The results showed that the proposed scheme outperformed traditional encryption algorithms in terms of security and efficiency levels.

Artificial neural networks (ANNs) have also been used in bioinspired encryption algorithms. ANNs are inspired by the biological neural networks in the human brain and have been used to optimize the encryption keys and improve the encryption quality. For instance, in [16, 17, 18], an ANN-based encryption scheme was proposed for WSNs, which showed improved performance compared to traditional encryption algorithms.

Chaos theory is another bioinspired approach used in encryption. Chaos theory is based on the concept of

deterministic chaos, which is characterized by sensitive dependence on initial conditions. Chaos theory has been used to enhance the randomness of encryption keys and improve the resistance to attacks. For example, in [19, 20], a chaos-based encryption scheme via DNA Coded Fuzzy (DNACF) was proposed for IoT networks, which showed improved security and energy efficiency compared to traditional encryption algorithms.

Hybrid bioinspired encryption algorithms that combine multiple bioinspired approaches have also been proposed for different use cases [21, 22, 23, 24]. These algorithms aim to improve the encryption quality and reduce the computational complexity and energy consumption of traditional encryption algorithms [25, 26]. For instance, in [27, 28, 29, 30], a hybrid bioinspired encryption algorithm was proposed for IoT networks, which combined GAs and chaotic maps to generate and optimize the encryption keys.

In summary, bioinspired encryption algorithms have shown promising results in enhancing the security of IoT networks. GAs, ANNs, chaos theory, and hybrid approaches have been proposed to optimize the encryption keys, enhance the randomness, and reduce the computational complexity and energy consumption of traditional encryption algorithms. However, further research is needed to optimize the performance of bioinspired encryption algorithms and ensure their scalability and interoperability in real-world IoT applications.

3. Proposed design of an efficient hybrid Bioinspired Encryption Model for enhancing Security of QoS-aware IoT Networks

As per the review of existing encryption models, it can be observed that researchers have proposed a wide variety of security optimization methods which maintain high QoS via dynamic programming techniques. But these techniques cannot be scaled for context-specific deployments, and cannot be reconfigured to support large-scale IoT (Internet of Things) Networks. To overcome these issues, this section proposes design of an efficient & Novel Elephant Herding Ant Lion Optimizer (EHALO), which assists in identification of security models & their internal configurations for different contextual deployments. As per figure 1, it can be observed that the proposed model integrates spatial security performance with temporal communication performance in order to decide which encryption model to use, and then fuses this information with temporal security measures in order to identify optimal security configurations.

As per figure 1, it can be observed that the model initially collects information about different encryption models, and their meta data samples. These contain various key combinations, ranges for different parameters, their existing temporal performance when applied to real-time networks, and execution metrics.

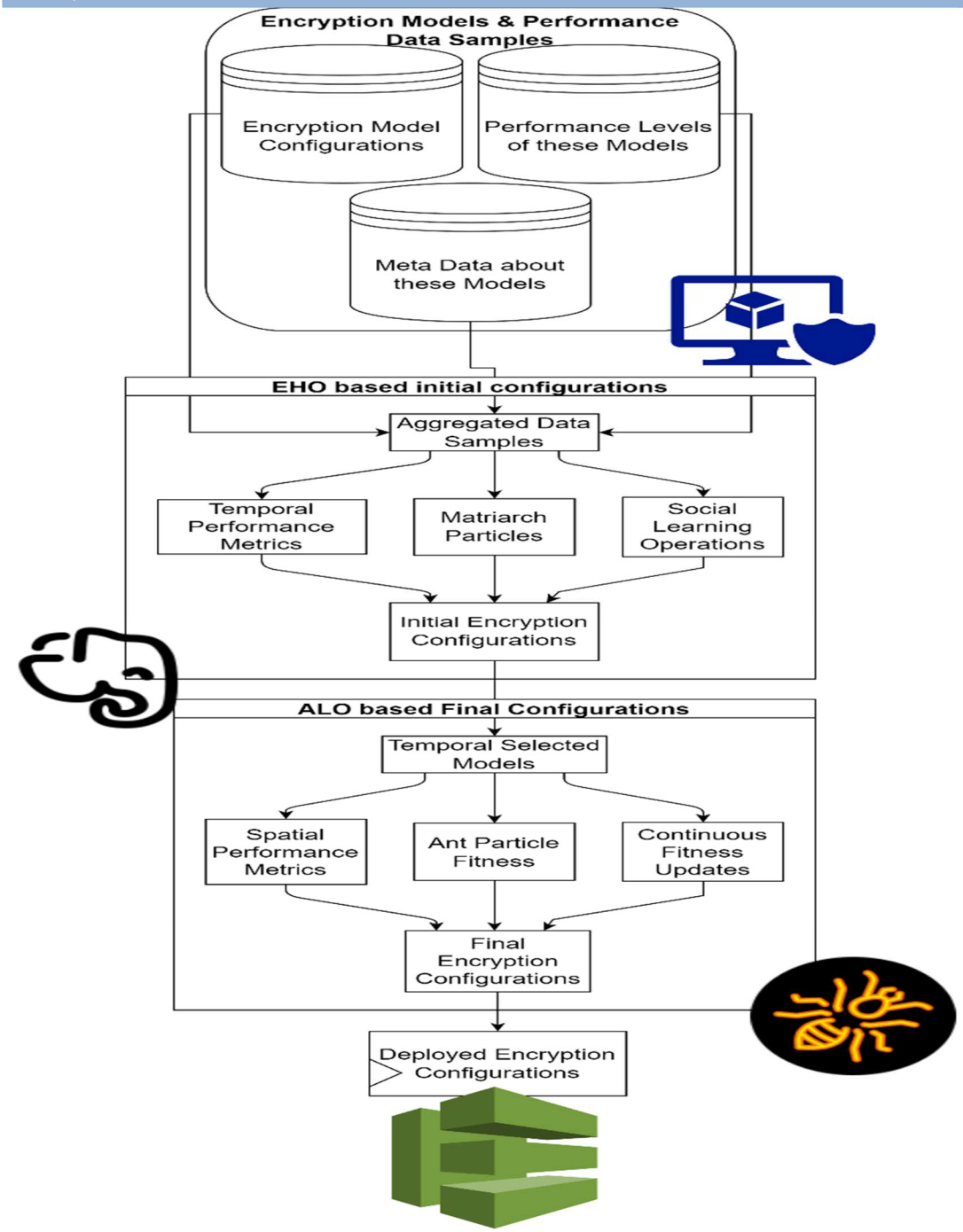

Figure 1. Design of the proposed hybrid bioinspired encryption process

To select an encryption model, an Elephant Herding Optimization (EHO) is used, which works as per the following process,

- A set of initial NE Number of Elephant Herds are initialized by stochastically selecting encryption models via equation 1,

$$N = STOCH\big(1, N(Enc)\big) \dots (1)$$

Where, $N, \& N(Enc)$ represents total number of encryption models selected, and total number of encryption models available, $N(Enc) \in (AES, DES, ECC, RSA)$, while $STOCH$ represents a stochastic process used for generation of number sets.

- Based on these encryption models, fitness function is estimated for this Herd via equation 2,

$$fh = \frac{1}{N}\sum_{i=1}^{N} PDR_i * \left(\frac{D_i}{Max(D)} + \frac{Max(THR)}{THR_i} + \frac{E_i}{Max(E)}\right) \dots (2)$$

Where, fh represents Herd fitness $PDR, D, THR \,\&\, E$ are temporal evaluation metrics for the given encryption models, and represent values for Packet Delivery Ratio, Delay, Throughput, and Energy Consumption levels. The PDR levels are estimated via equation 3,

$$PDR = \frac{1}{NC}\sum_{i=1}^{NC} \frac{P_{rx_i}}{P_{tx_i}} \dots (3)$$

Where, P_{rx} & P_{tx} represents the packets received and transmitted during NC temporal communications. Similarly, the delay is estimated via equation 4,

$$D = \frac{1}{NC}\sum_{i=1}^{NC} TS_{complete_i} - TS_{start_i} \dots (4)$$

Where, TS represents timestamps for completing and starting the communication operations. Based on these metrics, the temporal throughput is estimated via equation 5,

$$THR = \frac{1}{NC}\sum_{i=1}^{NC} \frac{P_{rx_i}}{D_i} \dots (5)$$

Along with this, the energy levels were estimated via equation 6,

$$E = \frac{1}{NC}\sum_{i=1}^{NC} E_{start_i} - E_{complete_i} \dots (6)$$

- This process is repeated for NE Herds, to evaluate different encryption configurations
- These configurations are used to estimate a Herd fitness threshold via equation 7,

$$fth = \frac{1}{NE}\sum_{i=1}^{NE} fh_i * LE \dots (7)$$

Where, LE represents learning rate for the EHO process.

- Herd with maximum fitness is marked as 'Matriarch' Herd, and is used to train other Herds that have fitness $fh < f_{th}$
- For such Herds, the internal configuration is modified via equation 8,

$$C(New) = C(Old) \cup \; STOCH\big(C(Matriarch)\big) \dots (8)$$

Where, C represents Herd Configurations.

- This process is repeated for NI Iterations, and new Herds are continuously reconfigured via different encryption combinations.

At the end of NI Iterations, configurations of the 'Matriarch' Herd are used, and the selected encryption models are further evaluated via an Ant Lion Optimization process. This process aims at optimizing temporal performance of the selected encryption model, and works as follows,

- To initialize the ALO Process, a set of NA Ants are generated via equation 9,

$$AC = \cup_{i=1}^{NE(EHO)} \cup_{j=1}^{NC(i)} STOCH(EC(j)) \dots (9)$$

Where, AC represents configuration of the Ant, while $NE(EHO)$ represents number of encryption models selected by the EHO process,
NC represents number of configuration parameters possible for the selected encryption model (key size, curve type, etc.)
while EC represents the encryption configuration parameter sets.

- Based on the selected Ant Configuration, its fitness is estimated via equation 10,

$$f_a = \frac{1}{N(AC)} \sum_{i=1}^{N(AC)} \left(\frac{D_i}{Max(D)} + \frac{Max(THR)}{THR_i} + \frac{E_i}{Max(E)} \right) \dots (10)$$

Where, $N(AC)$ represents Number of Ant Configurations used for the evaluation process.

- These values are estimated for Spatial processes, and assist in identification of optimal encryption parameters for the selected methods.

- Based on these values, an iteration fitness is estimated for all Ants via equation 11,

$$f_{th} = \frac{1}{NA} \sum_{i=1}^{NA} f_a(i) * LA \dots (11)$$

Where, NA are total Number of Ants, while LA represents their learning rate levels.

Before starting the next iteration, check if $f_a \leq f_{th}$ for any given set of Ants.

Mark these Ants as 'AntLions' and pass them directly to the next set of iterations.

Discard other Ants, and replace them with new Ants in consecutive iterations.

After this process is repeated for NI Iterations, select the Ant with minimum fitness levels. The configuration of this Ant will be used to perform high-efficiency encryption while maintaining high security levels. To validate this performance, the model was evaluated in terms of different QoS Parameters, and compared with existing methods in the next section of this text.

4. Result analysis & comparison

The proposed model aims to improve the overall security of communication networks by integrating spatial security performance with temporal communication performance. This integration enables the selection of appropriate encryption models based on the combination of both spatial and temporal performance measures, which are then combined with temporal security measures to determine optimal security configurations. The model was evaluated using various data level attack scenarios, including Spoofing, Grey Hole, and Masquerading & Man-in-the-Middle (MITM) attacks.

To evaluate the effectiveness of the proposed model, it was tested under several types of attacks, including Sybil, spoofing, distributed denial of service (DDoS), and masquerading scenarios. A Network Simulator was used to conduct the evaluation, and the parameters listed in table 1 were initialized following specific procedures for each set of individual evaluations.

The proposed model's effectiveness was assessed by measuring its ability to identify optimal security configurations that can withstand these attacks. The results of the evaluation demonstrate the model's effectiveness in identifying such configurations and its ability to improve the overall security of communication networks.

Network Parameter Sets	**Empirical Values for the given Parameter Sets**
Mode used for the Antenna	Dual Rays with Omnidirectional Modes
MAC Model	802.16a
Total count of nodes in the Network	15k
Default Routing Model	AOMDV (Adhoc On-Demand Multipath Distance Vector Routing Process)
Width & Length of the Network	4.5km x 4.5km
Energy Model	
Power needed by node when it's in reception mode	Idle: 0.001 mW Reception: 1.25 mW Transmission: 2.5 mW Sleep: 0.00005 mW Transition: 0.0025 mW Initial: 500 mW
Delay during Transitions	0.0025 s

Table 1. Simulation Parameters used for evaluation of performance for the proposed model under different attacks

Several metrics, including communication delay (D), energy consumption (E), throughput (THR), and packet delivery ratio (PDR), were compared for various values of these parameters within the simulation in order to assess the performance of the proposed model. These metrics were assessed for a variety of Numbers of Communications under the premise that random attacks would make up 10% of all NC communications.

A dataset of 1.5 million requests was used to test the proposed model, and its outcomes were compared with those of three additional models, namely CNOM [3], MKHE [13], and DNA CF [19], using the same simulation parameters & scenarios. The performance of the suggested model was evaluated using this methodology for different scenarios.

The amount of time needed for communication was ascertained and shown in Table 2 based on the evaluation technique used. The results indicate that even in the presence of random attacks, the proposed model can maintain effective communication under a range of communication delay, energy consumption, throughput, and packet delivery ratio conditions.

NC	D (ms) CNOM [3]	D (ms) MKHE [13]	D (ms) DNA CF [19]	D (ms) BMEH CQS
75k	17.08	13.23	14.86	9.95
150k	19.50	15.09	16.92	11.29
225k	22.02	17.03	19.07	12.69
300k	24.57	19.01	21.25	14.09
375k	27.05	20.96	23.40	15.46
450k	29.40	22.83	25.47	16.78
525k	31.62	24.63	27.46	18.05
600k	33.75	26.34	29.36	19.26
675k	35.82	28.02	31.22	20.46
750k	37.93	29.70	33.09	21.67
1M	40.10	31.41	35.00	22.91
1.05M	42.37	33.19	36.97	24.18
1.12M	44.70	35.01	38.98	25.49
1.3M	47.07	36.87	41.04	26.82
1.4M	49.45	38.74	43.11	28.15
15M	51.81	40.59	45.16	29.48

Table 2. Delay needed to perform communications by using the proposed model under attacks

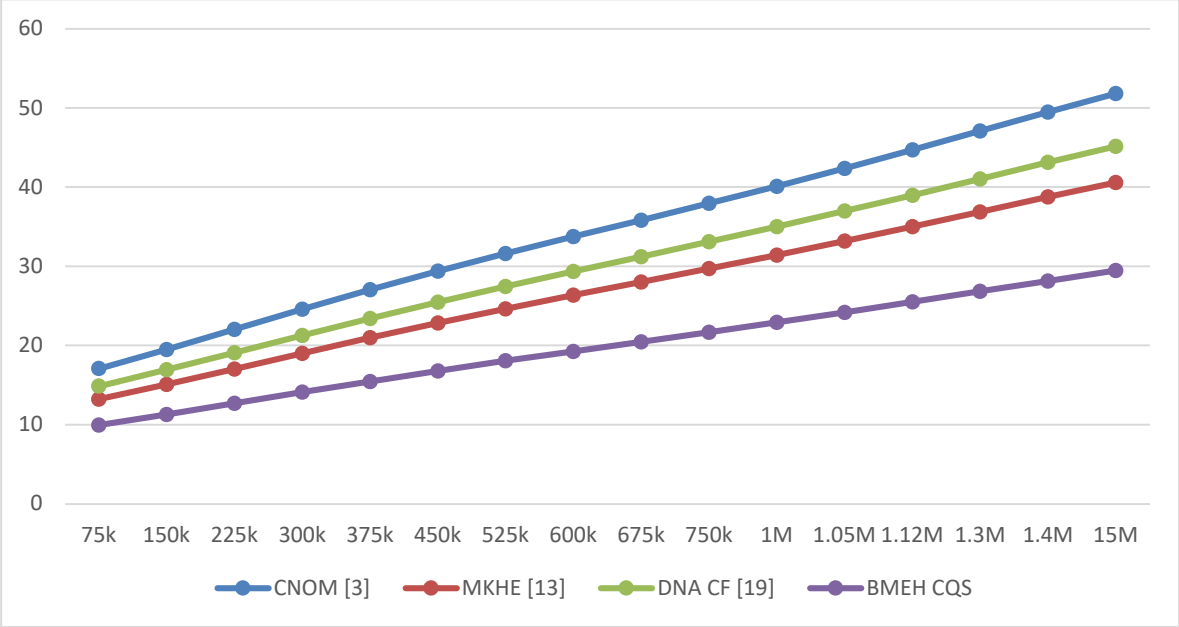

Figure 2. Delay needed to perform communications by using the proposed model under attacks

As per this evaluation and its visualization in figure 2, it can be observed that the proposed model is able to reduce communication delay by 24.5% when compared with CNOM [3], 18.5% when compared with MKHE [13], and 19.4% when compared with DNA CF [19] under different attacks. This delay is reduced due to selection of delay-aware encryption models via the EHO Process, and selection of QoS-aware hyperparameters via the ALO process. Due to this performance, the proposed model is highly useful for delay-aware security deployments & scenarios. Similarly, the energy needed for these operations can be observed from table 3 as follows,

NC	**E (mJ) CNOM [3]**	**E (mJ) MKHE [13]**	**E (mJ) DNA CF [19]**	**E (mJ) BMEH CQS**
75k	27.65	27.33	24.43	16.59
150k	28.95	28.63	25.58	17.36
225k	30.28	29.94	26.74	18.14
300k	31.65	31.26	27.89	18.91
375k	33.02	32.58	29.04	19.68
450k	34.40	33.87	30.17	20.43
525k	35.76	35.15	31.29	21.18

600k	37.11	36.42	32.39	21.92
675k	38.43	37.68	33.49	22.66
750k	39.74	38.94	34.61	23.41
1M	41.05	40.21	35.72	24.16
1.05M	42.37	41.50	36.86	24.92
1.12M	43.70	42.79	37.99	25.68
1.3M	45.04	44.08	39.13	26.44
1.4M	46.38	45.38	40.26	27.21
1.5M	47.72	46.68	41.40	27.97

Table 3. Energy needed to perform communications by using the proposed model under attacks

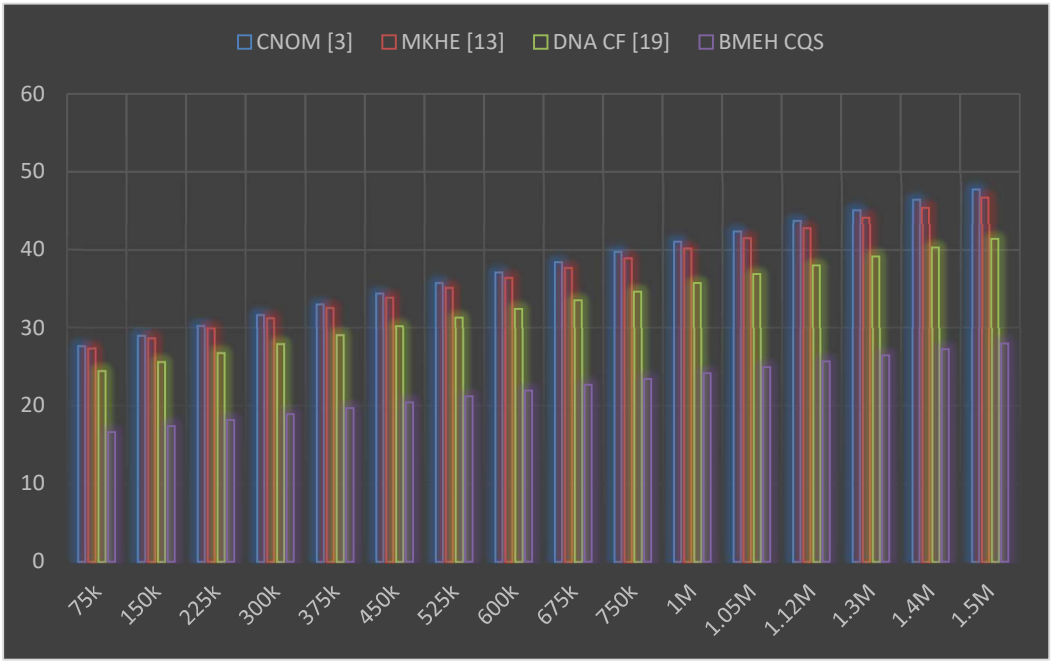

Figure 3. Energy needed to perform communications by using the proposed model under attacks

When compared to CNOM [3], MKHE [13], and [R3 under various attacks, the proposed model is able to reduce the energy required for communication by 38.4%, 35.5%, and 32.5%, respectively, according to this evaluation and its visualization in figure 3. By choosing encryption models that respect QoS through the EHO Process and choosing energy-conscious hyperparameters through the ALO Process, this energy is reduced. This performance

makes the suggested model very helpful for energy-conscious security deployments and scenarios. Similar to that, table 4 shows the throughput required (or attained) during these operations as follows,

NC	T (kbps) CNOM [3]	T (kbps) MKHE [13]	T (kbps) DNA CF [19]	T (kbps) BMEH CQS
75k	2507	1729	2029	2730
150k	2527	1743	2045	2752
225k	2548	1757	2062	2775
300k	2569	1771	2079	2797
375k	2589	1785	2095	2819
450k	2609	1799	2111	2841
525k	2630	1813	2128	2863
600k	2650	1827	2144	2885
675k	2671	1841	2161	2907
750k	2691	1855	2177	2929
1M	2712	1869	2194	2952
1.05M	2733	1883	2210	2974
1.12M	2753	1898	2227	2996
1.3M	2774	1912	2244	3018
1.4M	2794	1926	2260	3040
1.5M	2815	1940	2277	3062

Table 4. Throughput needed (or obtained) while perform communications by using the proposed model under attacks

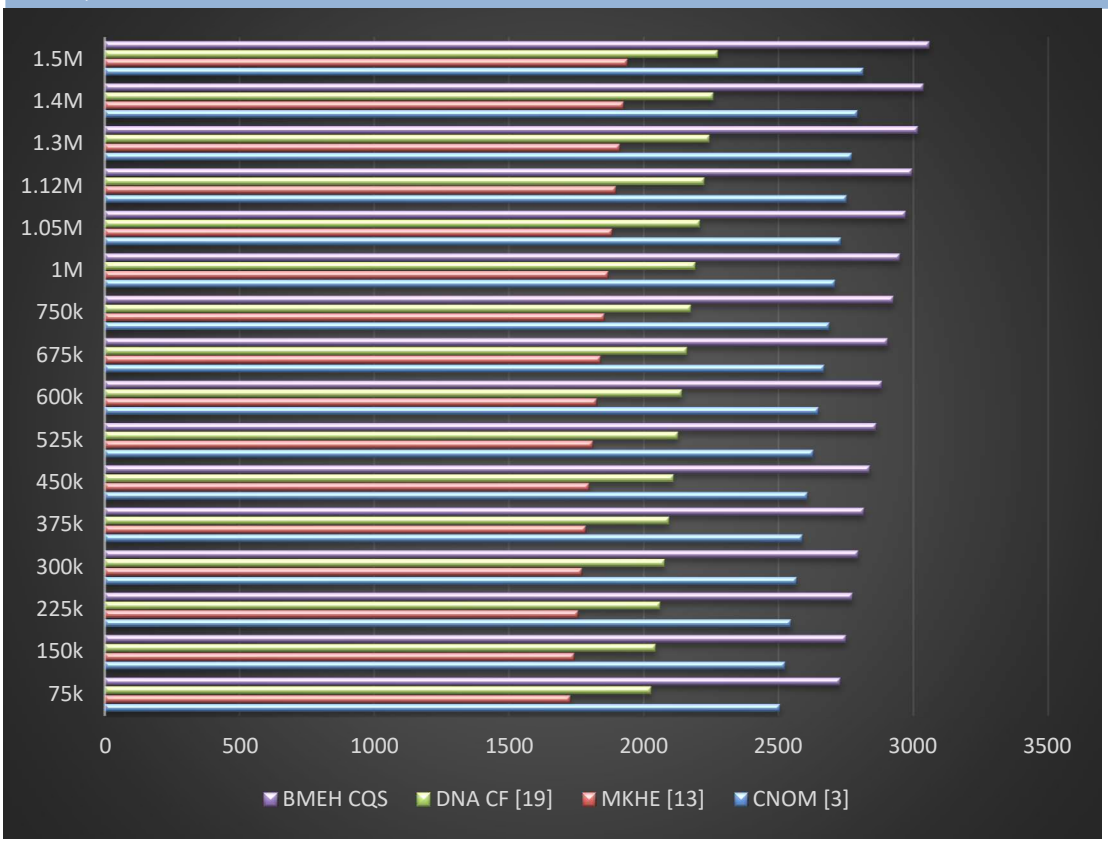

Figure 4. Throughput needed (or obtained) while perform communications by using the proposed model under attacks

According to this evaluation and its visualization in figure 4, it can be seen that the proposed model is able to improve the throughput needed during communications by 8.3% when compared with CNOM [3], 14.5% when compared with MKHE [13], and 12.5% when compared with DNA CF [19] under various attacks. This improvement can be attributed to the fact that the proposed model is capable of reducing the amount of time that is spent waiting for data to be transmitted. This throughput has increased as a result of the selection of encryption models that are data-rate-aware through the EHO Process and selection of quality-of-service aware hyperparameters through the ALO Process. As a result of this performance, the model that was proposed is extremely helpful for data-rate-aware security deployments and scenarios. In a similar vein, the PDR that was required (or attained) throughout these operations can be seen, as shown in table 5, as follows,

NC	**PDR (%) CNOM [3]**	**PDR (%) MKHE [13]**	**PDR (%) DNA CF [19]**	**PDR (%) BMEH CQS**
75k	84.29	79.84	82.54	88.92
150k	85.11	80.58	83.30	89.65
225k	85.92	81.31	84.05	90.38

300k	86.74	82.05	84.81	91.12
375k	87.55	82.78	85.56	91.85
450k	88.36	83.51	86.31	92.58
525k	89.18	84.24	87.06	93.31
600k	89.99	84.97	87.81	94.03
675k	90.80	85.70	88.56	94.76
750k	91.61	86.43	89.31	95.48
1M	92.43	87.17	90.07	96.21
1.05M	93.24	87.90	90.82	96.93
1.12M	94.05	88.63	91.58	97.66
1.3M	94.87	89.37	92.33	98.39
1.4M	95.68	90.10	93.08	99.12
1.5M	96.50	90.83	93.83	99.85

Table 5. PDR needed (or obtained) while perform communications by using the proposed model under attacks

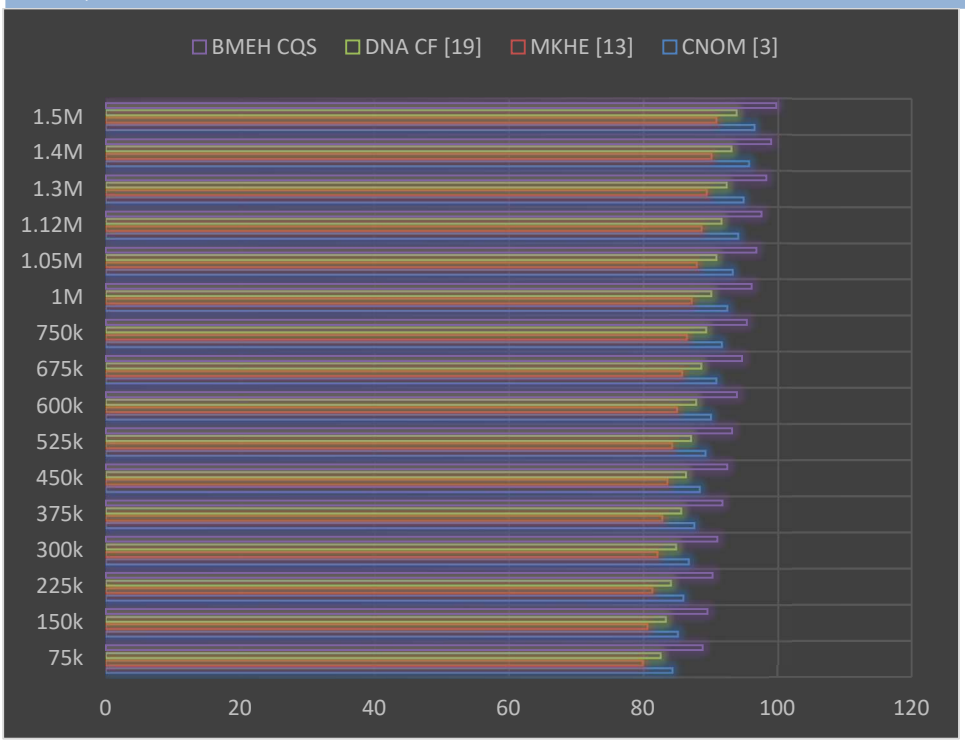

Figure 5. PDR needed (or obtained) while perform communications by using the proposed model under attacks

Based on the results of this analysis, which are depicted in figure 5, it is clear that the proposed model reduces the amount of PDR required for communications with attacks from CNOM [3] by 3.5 percentage points, from MKHE [13] by 8.3 percentage points, and from DNA CF [19] by 4.5 percentage points. Selecting consistency-aware encryption models via the EHO Process and PDR-aware hyperparameters via the ALO Process both contribute to the enhancement of this PDR. The proposed model's robustness makes it ideal for applications and settings where security consistency is of paramount importance. These improvements allow the proposed model to improve throughput and maintain consistency in packet delivery across extensive communications while reducing energy consumption for real-time scenarios.

5. Conclusion and future scope

By fusing spatial security performance with temporal communication performance, the suggested model seeks to increase the overall security of communication networks. By combining spatial and temporal performance measures, this integration makes it possible to choose the best encryption models, which are then combined with temporal security measures to produce the best security configurations. Different data level attack scenarios, such as spoofing, grey hole, masquerading, and man-in-the-middle (MITM) attacks, were used to evaluate the model. The proposed model was put to the test against a variety of attacks, including Sybil, spoofing, distributed denial of service (DDoS), and masquerading scenarios, in order to gauge its effectiveness. The effectiveness of the suggested model was measured by how well it could pinpoint the best security setups that could fend off these assaults. The evaluation's findings show how well the model works at spotting these configurations and how it can raise communication networks' overall security.

According to this assessment, it was found that the proposed model can reduce communication delay under various attacks by 24.5% when compared to CNOM [3], 18.5% when compared to MKHE [13], and 19.4% when compared to DNA CF [19]. The EHO Process and the ALO Process are used to select QoS-aware hyper parameters and delay-aware encryption models. This performance makes the suggested model extremely helpful for

deployments and scenarios involving delay-aware security levels. These evaluations show that the proposed model can reduce the energy needed for communication by 38.4%, 35.5%, and 32.5%, respectively. This energy is decreased by selecting encryption models that respect QoS through the EHO Process and selecting energy-conscious hyper parameters through the ALO Process. The suggested model's performance makes it very beneficial for energy-conscious security deployments and scenarios.

It is clear that the suggested model, when compared to CNOM [3], MKHE [13], and DNA CF [19], can increase the throughput required for communications by 8.3%, 14.5%, and 12.5%, respectively, under different attacks. This improvement can be attributed to the proposed model's ability to decrease the amount of time needed in various scenarios to wait for data transmission. This throughput has increased as a result of the EHO Process's selection of encryption models that take data rate considerations into account and the ALO Process's selection of hyper parameters that take quality of service considerations for different scenarios. This performance makes the suggested model very valuable for data-rate-aware security deployments and scenarios. The amount of PDR needed for communications with attacks from CNOM [3] drops by 3.5 percentage points, MKHE [13] drops by 8.3 percentage points, and DNA CF [19] drops by 4.5 percentage points according to the proposed model. This PDR is improved by choosing consistency-aware encryption models through the EHO Process and PDR-aware hyper parameters through the ALO Process. Because of its robustness, the proposed model is perfect for use in situations and applications where security consistency is crucial. These enhancements enable the proposed model to reduce energy consumption for real-time scenarios, increase throughput, and maintain consistency in packet delivery across extensive communications.

Future Scopes

The following can be future scopes of this work,

1. Integration with blockchain technology: The integration of the proposed encryption model with block chain technology can enhance the security of IoT networks by providing an immutable and tamper-proof ledger that ensures secure communication and data exchange scenarios.

2. Implementation in real-time IoT systems: The proposed encryption model can be implemented in real-time IoT systems to enhance the security of these systems, which can have numerous applications in fields such as healthcare, transportation, and smart cities.

3. Development of new bioinspired algorithms: The proposed encryption model uses bioinspired algorithms such as the genetic algorithm and artificial neural networks. Further research can explore the development of new bioinspired algorithms to improve the efficiency and effectiveness of the encryption models.

4. Application in other security systems: The proposed encryption model can be applied in other security systems beyond IoT networks, such as cloud computing and wireless sensor networks.

5. Evaluation of the proposed model's performance under different scenarios: The performance of the proposed encryption model can be evaluated under different scenarios such as network size, traffic patterns, and attack types to identify its effectiveness and limitations in various situations.

6. References

[1] M. Soltani, M. Kamal, A. Afzali-Kusha and M. Pedram, "An Adaptive Memory-Side Encryption Method for Improving Security and Lifetime of PCM-Based Main Memory," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 41, no. 6, pp. 1744-1756, June 2022, doi: 10.1109/TCAD.2021.3093832.

[2] P. N. Andono and D. R. I. M. Setiadi, "Improved Pixel and Bit Confusion-Diffusion Based on Mixed Chaos and Hash Operation for Image Encryption," in IEEE Access, vol. 10, pp. 115143-115156, 2022, doi: 10.1109/ACCESS.2022.3218886.
[3] Z. Hu, P. Song and C. -K. Chan, "Chaotic Non-Orthogonal Matrix-Based Encryption for Secure OFDM-PONs," in IEEE Photonics Technology Letters, vol. 33, no. 20, pp. 1127-1130, 15 Oct.15, 2021, doi: 10.1109/LPT.2021.3109029.
[4] Z. Hu, P. Song and C. -K. Chan, "Chaotic Non-Orthogonal Matrix-Based Encryption for Secure OFDM-PONs," in IEEE Photonics Technology Letters, vol. 33, no. 20, pp. 1127-1130, 15 Oct.15, 2021, doi: 10.1109/LPT.2021.3109029.
[5] Z. Hu, P. Song and C. -K. Chan, "Chaotic Non-Orthogonal Matrix-Based Encryption for Secure OFDM-PONs," in IEEE Photonics Technology Letters, vol. 33, no. 20, pp. 1127-1130, 15 Oct.15, 2021, doi: 10.1109/LPT.2021.3109029.
[6] B. Zhu, F. Wang and J. Yu, "A Chaotic Encryption Scheme in DMT for IM/DD Intra-Datacenter Interconnects," in IEEE Photonics Technology Letters, vol. 33, no. 8, pp. 383-386, 15 April15, 2021, doi: 10.1109/LPT.2021.3064582.
[7] L. Gao, L. Qi and L. Guan, "The Property of Frequency Shift in 2D-FRFT Domain With Application to Image Encryption," in IEEE Signal Processing Letters, vol. 28, pp. 185-189, 2021, doi: 10.1109/LSP.2021.3050052.
[8] Y. Chen, Y. Huang, J. Fu, Y. Han, K. Li and J. Yu, "Multi Wings Chaotic Encryption Scheme for PAM-DMT-Based Optical Access Network," in IEEE Photonics Journal, vol. 13, no. 1, pp. 1-8, Feb. 2021, Art no. 7900408, doi: 10.1109/JPHOT.2020.3047920.
[9] Y. Chen, Y. Huang, J. Fu, Y. Han, K. Li and J. Yu, "Multi Wings Chaotic Encryption Scheme for PAM-DMT-Based Optical Access Network," in IEEE Photonics Journal, vol. 13, no. 1, pp. 1-8, Feb. 2021, Art no. 7900408, doi: 10.1109/JPHOT.2020.3047920.
[10] Y. Chen, Y. Huang, J. Fu, Y. Han, K. Li and J. Yu, "Multi Wings Chaotic Encryption Scheme for PAM-DMT-Based Optical Access Network," in IEEE Photonics Journal, vol. 13, no. 1, pp. 1-8, Feb. 2021, Art no. 7900408, doi: 10.1109/JPHOT.2020.3047920.
[11] Y. Chen, Y. Huang, J. Fu, Y. Han, K. Li and J. Yu, "Multi Wings Chaotic Encryption Scheme for PAM-DMT-Based Optical Access Network," in IEEE Photonics Journal, vol. 13, no. 1, pp. 1-8, Feb. 2021, Art no. 7900408, doi: 10.1109/JPHOT.2020.3047920.
[12] Y. M. Al-Moliki, M. T. Alresheedi, Y. Al-Harthi and A. H. Alqahtani, "Robust Lightweight-Channel-Independent OFDM-Based Encryption Method for VLC-IoT Networks," in IEEE Internet of Things Journal, vol. 9, no. 6, pp. 4661-4676, 15 March15, 2022, doi: 10.1109/JIOT.2021.3107395.
[13] X. Yang, S. Zheng, T. Zhou, Y. Liu and X. Che, "Optimized relinearization algorithm of the multikey homomorphic encryption scheme," in Tsinghua Science and Technology, vol. 27, no. 3, pp. 642-652, June 2022, doi: 10.26599/TST.2021.9010047.
[14] C. Equihua et al., "A low-cost and highly compact FPGA-based encryption/decryption architecture for AES algorithm," in IEEE Latin America Transactions, vol. 19, no. 9, pp. 1443-1450, Sept. 2021, doi: 10.1109/TLA.2021.9468436.
[15] Z. Gao et al., "25 Gb/s Physical Secure Communication Based on Temporal Spreading-Then-Random Phase Encryption," in IEEE Photonics Technology Letters, vol. 33, no. 24, pp. 1363-1366, 15 Dec.15, 2021, doi: 10.1109/LPT.2021.3122510.
[16] Z. Gao et al., "25 Gb/s Physical Secure Communication Based on Temporal Spreading-Then-Random Phase Encryption," in IEEE Photonics Technology Letters, vol. 33, no. 24, pp. 1363-1366, 15 Dec.15, 2021, doi: 10.1109/LPT.2021.3122510.
[17] Y. Song, Q. Wu, X. Wang, C. Wang and X. Miao, "Two Memristors-Based XOR Logic Demonstrated With Encryption/Decryption," in IEEE Electron Device Letters, vol. 42, no. 9, pp. 1398-1401, Sept. 2021, doi: 10.1109/LED.2021.3102678.
[18] A. Al Badawi, Y. Polyakov, K. M. M. Aung, B. Veeravalli and K. Rohloff, "Implementation and Performance Evaluation of RNS Variants of the BFV Homomorphic Encryption Scheme," in IEEE Transactions

on Emerging Topics in Computing, vol. 9, no. 2, pp. 941-956, 1 April-June 2021, doi: 10.1109/TETC.2019.2902799.
[19] A. G. Mohamed, N. O. Korany and S. E. El-Khamy, "New DNA Coded Fuzzy Based (DNAFZ) S-Boxes: Application to Robust Image Encryption Using Hyper Chaotic Maps," in IEEE Access, vol. 9, pp. 14284-14305, 2021, doi: 10.1109/ACCESS.2021.3052161.
[20] A. Toktas, U. Erkan, F. Toktas and Z. Yetgın, "Chaotic Map Optimization for Image Encryption Using Triple Objective Differential Evolution Algorithm," in IEEE Access, vol. 9, pp. 127814-127832, 2021, doi: 10.1109/ACCESS.2021.3111691.
[21] L. Cheng and F. Meng, "Certificateless Public Key Authenticated Searchable Encryption With Enhanced Security Model in IIoT Applications," in IEEE Internet of Things Journal, vol. 10, no. 2, pp. 1391-1400, 15 Jan.15, 2023, doi: 10.1109/JIOT.2022.3207229.
[22] K. Shahbazi and S. -B. Ko, "Area-Efficient Nano-AES Implementation for Internet-of-Things Devices," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 29, no. 1, pp. 136-148, Jan. 2021, doi: 10.1109/TVLSI.2020.3033928.
[23] C. Yu, Z. Ding and X. Chen, "HOPE: Software Defect Prediction Model Construction Method via Homomorphic Encryption," in IEEE Access, vol. 9, pp. 69405-69417, 2021, doi: 10.1109/ACCESS.2021.3078265.
[24] X. Liu, A. G. Richardson and J. Van der Spiegel, "An Energy-Efficient Compressed Sensing-Based Encryption Scheme for Wireless Neural Recording," in IEEE Journal on Emerging and Selected Topics in Circuits and Systems, vol. 11, no. 2, pp. 405-414, June 2021, doi: 10.1109/JETCAS.2021.3074938.
[25] R. Parekh et al., "GeFL: Gradient Encryption-Aided Privacy Preserved Federated Learning for Autonomous Vehicles," in IEEE Access, vol. 11, pp. 1825-1839, 2023, doi: 10.1109/ACCESS.2023.3233983.
[26] E. Sarkar, E. Chielle, G. Gürsoy, O. Mazonka, M. Gerstein and M. Maniatakos, "Fast and Scalable Private Genotype Imputation Using Machine Learning and Partially Homomorphic Encryption," in IEEE Access, vol. 9, pp. 93097-93110, 2021, doi: 10.1109/ACCESS.2021.3093005.
[27] S. Chen, L. Li, W. Zhang, X. Chang and Z. Han, "BOPE: Boundary Order-Preserving Encryption Scheme in Relational Database System," in IEEE Access, vol. 9, pp. 30124-30134, 2021, doi: 10.1109/ACCESS.2021.3058186.
[28] S. Jumonji, K. Sakai, M. -T. Sun and W. -S. Ku, "Privacy-Preserving Collaborative Filtering Using Fully Homomorphic Encryption," in IEEE Transactions on Knowledge and Data Engineering, vol. 35, no. 3, pp. 2961-2974, 1 March 2023, doi: 10.1109/TKDE.2021.3115776.
[29] U. Hijawi, D. Unal, R. Hamila, A. Gastli and O. Ellabban, "Lightweight KPABE Architecture Enabled in Mesh Networked Resource-Constrained IoT Devices," in IEEE Access, vol. 9, pp. 5640-5650, 2021, doi: 10.1109/ACCESS.2020.3048192.
[30] P. Arpaia, F. Bonavolontà, A. Cioffi and N. Moccaldi, "Reproducibility Enhancement by Optimized Power Analysis Attacks in Vulnerability Assessment of IoT Transducers," in IEEE Transactions on Instrumentation and Measurement, vol. 70, pp. 1-8, 2021, Art no. 3523608, doi: 10.1109/TIM.2021.3107610.

[31]Implementation of Health Impact Assessment of Packaged Foods through Nutritional Label Recognition using OCR Guru, S., Bamane, K.D., Patankar, A., ... Katre, A., Vyavahare, D.*Frontiers in Health Informatics, 2024, 13(3), pp. 4783–4793[32]A critical analysis of crop management using Machine Learning towards smart and precise farming* Chaudhari, R.R., Bamane, K.D., Agrawal, H., . Gaikwad, A.S., Patankar, A.J.*Journal of Integrated Science and Technology, 2024, 12(5), 809*

[33]AI-Enabled Diagnostic Solution for Eye Disease Detection and Treatment Planning Sinkar, Y., Bamane, K.D., Chougale, M., Desai, L.R., Mane, D.P.*Frontiers in Health Informatics*, 2024, 13(3), pp. 4794–4810

[34] Innovative Healthcare Advancements: Harnessing Artificial and Human Intelligence for Bionic Solutions, Sapkal, S., Jadhav, S., Mallikarjun, P., ... Ul Islam, A., Bamane, K.
2024 OPJU International Technology Conference on Smart Computing for Innovation and Advancement in Industry 4.0, OTCON 2024, 2024