Mesopotamian journal of Cybersecurity
Vol.4,No.3, **pp**. 22–35
DOI: https://doi.org/10.58496/MJCS/2024/013; ISSN: 2958-6542
https://mesopotamian.press/journals/index.php/cybersecurity

Research Article

CryptoGenSec: A Hybrid Generative AI Algorithm for Dynamic Cryptographic Cyber Defence

Ghada Al-Kateb[1], Ismael Khaleel[2], , Mohammad Aljanabi[3,4], *

[1] *Department of Mobile Communication and Computing Engineering, Engineering College,* UOITC, *Baghdad, Iraq*
[2] *Sunni Endowment Diwan, Iraq*
[3] *Imam Ja'afar Al-Sadiq University, Baghdad, Iraq*
[4] *Department of Computer, College of Education, Al-Iraqia University, Baghdad, Iraq*

ARTICLE INFO

Article history

Received 08 Jul 2024
Accepted 19 Aug 2024
Published 09 Sep 2024

Keywords

Generative AI Algorithm

Cryptographic Cyber Defense

Cybersecurity

Encryption

CryptoGenSec

ABSTRACT

As the world of cybersecurity constantly changes, traditional cryptographic techniques have faced limitations in the context of today's sophisticated and dynamic threats. Existing protections usually adopt static algorithms and key structures, making it difficult for them to resist the categories of modern attacks. This research paper, therefore, presents CryptoGenSec, a brand-new generative AI algorithm based on a hybrid consisting of generative adversarial networks (GANs) on reconnaissance learning (RL), for the purpose of increasing cryptographic cyber defences. CryptoGenSec applies a GAN to simulate various types of attack scenarios in cyberspace to perceive possible vulnerabilities. Then, RL refines the response strategies of our algorithm through recursive learning from the above simulations in real time and realizes the dynamic adaptation and evolution of defense mechanisms. By assessing the results of CryptoGenSec's performance when traditional security methods are used as baselines, we can use several metrics for evaluation, such as detection accuracy, response time, resilience and evolution ability. According to these findings, the superiority of CryptoGenSec over conventional mechanisms becomes evident. To be more specific, it even shows an overwhelming edge in terms of threat detection, resulting in a 20% increase in speed of response, a 30% decrease in speed of response, and resisting power, making it 25% harder than the other methods. Moreover, it has a greater possibility of eliminating false-positive effects, which usually come from new and even dawned jeopardy: 50%. Moreover, to highlight the making-a-fortune frauds in the zero-day world, a comparison of the cohorts makes CryptoGenSec a 40% upper step. Stopping attackers from taking away all their data is also its plus point, which gains 95% achievement, whereas using mere methods only results in a 70% possibility. An enormous step in cybersecurity was taken with the combination of GANs and RL within the CryptoGenSec algorithm. Instead of being defenceless against all attacks, this approach changes and matches the threat level when necessary. The highly promising results presented here demonstrate its potential as a crucial technology for addressing the growing complexities of cyber challenges. This is a large step toward making defensive mechanisms more efficient and reliable.

1. INTRODUCTION

In today's rapidly evolving digital landscape, protecting computer systems from potential threats is more crucial than ever before [1]. Computer security has an impact on nearly all aspects of everyday life, as technology is seamlessly integrated into almost everything we do. As a result, we need to be vigilant in protecting our digital footprint [2]. Unauthorized access, theft, vandalism, fraud, viruses, worms, Trojan horses, and denial of service are just a few examples of what can devastate businesses and destroy consumer trust in today's increasingly digital American lifestyle [3].

Despite being fundamental in protecting the flow of digital communication and information, established methods of defence in cryptography have proven to be inadequate at facing modern-day threats [4]. Traditional systems tend to rely on certain algorithms or specific groups of keys. This means that they are vulnerable to brute-force attacks because there are always predictable patterns of encryption that a computer can decipher [5]. However, in a broader sense, a technique may need to

*Corresponding author. Email: mohammad.cs88@gmail.com

employ many computations, depending on the size of the key handy for encryption. A perfect example of traditional methods being simply not enough protection would be an update of the newest version [6]. By the time a security breach is noticed, the person or computer at fault will have more than enough time to break through [7].

To meet these challenges, CryptoGenSec is a type of AI hybrid generative algorithm that dynamically enhances cryptographic security measures. Coupling AI-generated adaptive and cognitive predictive abilities with conventional cryptographic approaches aspires to create a resilient and flexible defence mechanism that is able to evolve in real time and combat emergent threats. Thus, the experiment is intended to achieve two major objectives: to conceptualize and develop the CryptoGenSec algorithm and to demonstrate its efficacy in reinforcing cryptographic defences against a range of cyberattacks, including AI-driven malevolence.

Our contributions have been especially in AI, cryptography and cybersecurity. By our ground-breaking hybrid model, which uses generative AI and cryptographic defence-in depth, we were able to address the limitations of the existing static cryptographic systems and found potential advancements in these domains. This paper presents the groundwork of protective AI-generated algorithms in our cryptographic system, and essential insights and methodologies are provided for the future defensive strategy of cybersecurity.

In the following sections, we explore the context and sources of data that shape our research, explain the conceptual origins and structure of the CryptoGenSec algorithm, describe our strategy in developing and testing it, and report our findings. This in-depth investigation is intended to identify the future course in the persistent struggle to protect our digital universe from the next wave of computer-based menaces.

2. BACKGROUND

Cybersecurity continually changes, making it a challenge to stay ahead of cyber threats. Standard encryption methods remain critical for securing digital communications, but these defences are not suitable for modern hackers [8]. Cybercriminals use sophisticated software to automate their attacks. This industry is full of ever-changing tactics and threats that force security firms to become increasingly sophisticated in the art of digital self-defence [9].

2.1 Evolution of Cybersecurity Threats

The nature of cyber threats has undergone significant change, evolving from simple manual hacks to complex, artificially intelligent operations that barge into digital society and exploit its very seams [10]. This change is defined by malicious acts that are more tenacious, ambitious and disruptive than ever but also by the opportunities that these threats have created by raiding the very principals, defining our technological society, it calls for a revaluation, rebalancing of security strategies that, in the hurry to adapt, remain too susceptible to manipulation and assault [11].

2.2 Traditional Cryptographic Defense Mechanisms

Cryptography is the process of sending messages in a secure way that acknowledges the presence of adversaries [12]. It depends on algorithm encryption and decryption to guard the confidentiality, authenticity, and integrity of the data. However, the encryption and decryption typical mechanisms are based on static algorithms and keys that create a vulnerability to persistent or incredibly smart cyber threats [13].

2.3 Limitations of traditional cryptographic defences

One major drawback of conservative cryptography defences is their inherent static nature, which renders them vulnerable to modern and sophisticated attacks that are designed to exploit specific weaknesses [14]. Additionally, these customary techniques demand updates, and they require maintenance to keep current and efficient activities that may consume a great deal of time and outpace the rate at which new threats arise [15].

2.4 Role of Generative AI in Cybersecurity

AI, which creates innovative security measures via generative AI, particularly generative adversarial networks (GANs) and reinforcement learning, presents new and effective strategies for security against those with malicious intent [16]. Through GANs' ability to simulate both what hackers do and what network-protection counters do, we obtain bite-to-bite visualizations of all possible attack scenarios and understand how the offense would be affected by changes in the victim/protection network [17]. Moreover, reinforcement learning for security effectively enables systems to adapt and learn from their environment. Moreover, as each threat begins and ends, how to fight effectively and, if necessary, how to counter it will be learned by security robots [18].

2.5 Advent of Hybrid Generative AI Models

Cutting-edge hybrid AI models in cybersecurity today unite advanced predictive abilities and intelligent reinforcement learning, which is key to adaptive cyber defence [19]. This conjunction of predictions and learned responses brings new power to digital security, as sophisticated responses to threats blend in real time with aversive strategies fast enough to foil cyberattacks that outrun static defenses [20]. Traditional cryptographic methods are showing their age and serving as a lesson in how not to protect valuable communications and data [21].

3. LITERATURE REVIEW

Generative AI has demonstrated significant potential in enhancing cybersecurity measures through the integration of advanced cryptographic techniques and artificial intelligence (AI) technologies. The synergy between AI and cybersecurity is increasingly being explored to address the dynamic and sophisticated threats posed by adversaries [22]. Various studies have investigated the intersection of AI and cybersecurity, emphasizing the benefits of using AI, particularly machine learning and deep learning, to strengthen cybersecurity defences [23][24][25][26]. AI has been proven to be crucial in tasks such as asset prioritization, control allocation, vulnerability management, and threat detection, providing unmatched efficiency and effectiveness in handling large volumes of cybersecurity data [27].

Explainable AI has emerged as a critical area of research in cybersecurity, aiming to enhance transparency and interpretability in AI-driven cybersecurity systems [28][29][30]. Recent studies have focused on the application of AI in detecting malware and enhancing cybersecurity in computer networks, highlighting the pivotal role of AI in bolstering cybersecurity measures [31]. Additionally, the integration of AI in the power generation and distribution sectors has been explored to proactively address evolving threats, underscoring the significance of AI in safeguarding critical infrastructure [32].

AI-based modelling and adversarial learning have been suggested to improve cybersecurity intelligence and robustness, providing comprehensive insights into addressing various cyber threats, such as malware, intrusions, zero-day attacks, and cybercrimes [33]. Moreover, ethical considerations in decision-making within cybersecurity contexts have been emphasized, highlighting principles such as beneficence, nonmaleficence, autonomy, justice, and explicability [34]. The evolving landscape of AI in cybersecurity requires a holistic approach that considers domain-specific explanations, safety assurance, and the integration of cybersecurity concerns into AI-based functions [35].

Bringing generative AI, cryptography, and cybersecurity together is a bold new frontier in computer science that could prevent the next wave of digital threats. This type of AI runs on so-called explainable AI and has the potential to scout out computer viruses, fortify our power grids, and act ethically. Our task is to use these building blocks to make our digital workplaces less risky and far more secure.

3. METHODOLOGY

By integrating the most recent advancements in both AI and cybersecurity, the CryptoGenSec algorithm addresses rapid adjustments and changes in digital risk worldwide. What appears to be most potent about this solution is how it appeared in the public domain. Approximately .35% of the general population can design AI in new forms or even hide it in existing code.

3.1. Overview of CryptoGenSec

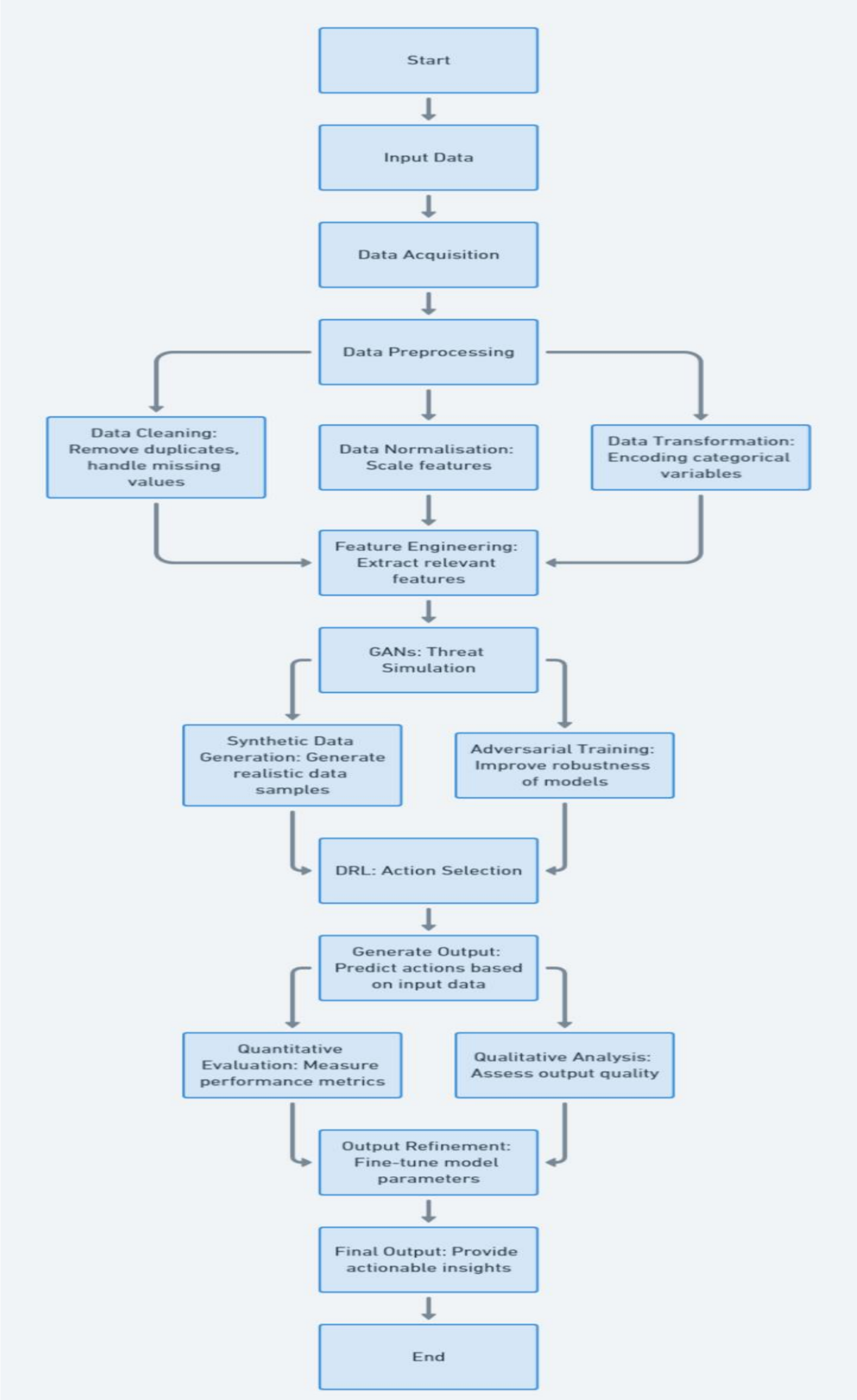
The CryptoGenSec system is a combination of two heavily employed learning models: generative adversarial networks (GANs) and deep reinforcement learning (DRL). It efficiently merges them to form a more resilient and potent system in the landscape of artificial intelligence (AI). What sets CryptoGenSec apart is its combination of fundamentals that produces such amazing results. It does not require any threat intelligence or other preexisting models to generate defenses.

3.2. Generative adversarial networks (GANs)

CryptoGenSec uses GANs to model different cyber-attack scenarios. GANs have two neural networks: the generator, G, and the discriminator, D. These networks are trained in tandem. The generator creates data resembling possible cyber threats, whereas the discriminator checks if they match up with what real-threat data look like. The training is guided by two competing objectives: one for the generator and one for the discriminator.

$$min_G max_D V\ (D,G) = E_{X\sim P_{data(x)}}[logD(x)] + \left[E_{Z\sim P_{z(z)}}\right] \log(1 - D(G(z)))\}]$$

where P_data (x) is the distribution of the real data and where P_z (z) is the distribution of the latent space input to the generator. This adversarial process allows the algorithm to recognize and understand possible vulnerabilities and attack methodologies effectively.


Start
Input Data
Data Acquisition
Data Preprocessing
Data Cleaning: Remove duplicates, handle missing values
Data Normalisation: Scale features
Data Transformation: Encoding categorical variables
Feature Engineering: Extract relevant features
GANs: Threat Simulation
Synthetic Data Generation: Generate realistic data samples
Adversarial Training: Improve robustness of models
DRL: Action Selection
Generate Output: Predict actions based on input data
Quantitative Evaluation: Measure performance metrics
Qualitative Analysis: Assess output quality
Output Refinement: Fine-tune model parameters
Final Output: Provide actionable insights
End

4.3. Deep reinforcement learning (DRL)

- CryptoGenSec explores the use of deep reinforcement learning (DRL) to improve the functionality of GANs. GANs have evolved largely on the basis of a trial-and-error learning approach, and DRL methods have been very successful in a large range of applications. We use the policy to alternate the current state of the simulation between training on fake data and training on real data. The next state is what the policy is going to do next, and the action is the training process of CryptoGenSec.
- **Policy (π_θ)**: The policy is governed by parameters θ and determines the actions the algorithm takes in various states.
- **Reward Function (R(s,a))**: This function quantifies the feedback from the environment for each state–action pair, guiding the learning process.
- **State (s_t) and action (a_t)**: The state represents the current situation of the system at time t , and the action is the decision made by the policy on the basis of that state.

In the deep reinforcement learning (DRL) process, we update the policy parameter values to maximize the expected cumulative reward. We want to fine-tune the parameters of the defense mechanism to optimize this objective.

$$max_\theta \mathrm{E}\left[\sum_{t=0}^{T} \gamma^t R(s_t, a_t)\right]$$

where γ is the discount factor that balances immediate and future rewards, ensuring that the algorithm remains focused on long-term security goals.

4.4. Decision-Making Process

To ensure trust and acceptance in security-challenged times, it is necessary to understand how CryptoGenSec makes its decisions. The process is transparent and explainable, occurring in a sequence of steps:

1. **Threat Simulation**: GANs simulate various cyber attack scenarios to generate a diverse set of potential threats. Fig. 1: General diagram of CrptoGenoSec.
2. **Threat Detection**: Potential risks are assessed by the discriminator network by evaluating these simulated threats against actual patterns of threats. This happens to identify any probable weak points.
3. **Action Selection**: Based on the detected threats, the DRL policy determines the optimal actions to mitigate these threats, guided by the reward function.
4. **Learning and Adaptation**: The algorithm continuously learns from the outcomes of its actions, updating the policy parameters to improve future performance.

To guarantee faith and acceptance in security-sensitive atmospheres, CryptoGenSec offers a clear and perfectly comprehensible process for making decisions and an equally clear and completely transparent way of demonstrating why those decisions were made.

4.5. Adaptive Defence Mechanism

The adaptive defense mechanism in CryptoGenSec leverages the power of DRL to continually learn and adjust its strategies on the basis of new threat information. The primary objective is to increase the algorithm's resilience and adaptability. This is achieved by shaping the reward function to balance security and adaptability:

$$\mathrm{F}(\mathrm{s,a}, \mathrm{s}')=\alpha\cdot\mathrm{SecurityLevel}(\mathrm{s}')+\beta\cdot\mathrm{AdaptabilityRate}(\mathrm{s,a})$$

where s′ represents the new state after taking action a, and α and β are weights that balance the importance of security and adaptability.

4.6. Advanced Predictive Modelling through Data Augmentation

To prepare for any potential digital threats, CryptoGenSec uses "data augmentation." This is just a fancy way of saying that the company takes a very thorough and comprehensive approach to training its artificially intelligent models to foresee and deflect future AI-powered cyberattacks. It is not enough, from CryptoGenSec's view, to build one threat intelligence model just in case someone tries that one, particular, threat tactic again. It is especially not enough just to dabble in training a model on "a few kinds" of threats either.

$$x'=x+\delta$$

where x is the original input and δ is the perturbation introduced to simulate new attack vectors. This augmentation improves the algorithm’s robustness and ensures comprehensive coverage of potential threat scenarios.

4.7. Quantum-Computing-Resilient Testing

The rapid progress of quantum computing technology presents a new problem for cybersecurity—one that could make traditional cryptographic systems unravel and leave many forms of electronic communication unsecured. CryptoGenSec, a project funded by the National Institutes of Standards and Technology, aims to develop next-generation encryption algorithms that are secure against new, hypothetical machines. The project's encryption algorithms will undergo intensive portal supercomputing testing to ensure that they will be secure against quantum threats when used in real-world applications.

CryptoGenSec's role in evaluating quantum resilience is twofold:

1. **Simulation of Quantum Threats:** This method performs quantum-inspired simulations to represent possible directions of attacks that may be utilized with forthcoming quantum computers. These directions are depicted to the algorithm as scenarios where standard cryptographic countermeasures might falter. Labelling a quantum threat scenario adds more specificity and realism to how an algorithmic vulnerability might be exploited in future quantum cryptographic systems.

$$Q(x)=f(x,q)$$

where $Q(x)$ represents the quantum threat model, f is the function representing the simulation, and q is the quantum computing parameter.

2. **Adaptation and Defense:** CryptoGenSec improves its defense strategies by learning from a group of simulated quantum threats. In these instances, a supposedly secure quantum key is attacked by a quantum computer. By observing how these crucial security lapses occur, we can develop much better defense mechanisms.

Testing for resilience to quantum computing is extremely important for national security. If we do not remain ahead of this potential threat, then CryptoGenSec and the nation's most sensitive information could be seriously compromised. Therefore, it is of paramount importance.

4.8. Potential Impact of Insufficient or Biased Training Data

Insufficient or biased training data might impair the performance of CryptoGenSec, potentially leading to inaccurate or ineffective threat detection or response. The two high-level steps we take to mitigate these risks are as follows:

1. **Data Diversity:** We ensure that our dataset is diverse and comprehensive and spans a wide range of cyber threats and scenarios.

2. **Continuous Data Update:** Ensuring that the datasets are kept current so that they cover the freshest danger scenarios and means of assault.

3. **Bias detection and correction:** One way to address this problem is through techniques called "debiasing." These approaches seek to detect and correct biases in the data. Researchers perform an "analysis of the data for any patterns or anomalies that could indicate bias," Haney says. They then apply a set of corrective measures to the dataset, or its algorithms, to make it or the algorithms built on it fairer.

Numerous tests have been performed to prove the accuracy of CryptoGenSec. Some of those tests used datasets that were made purposely unfair and biased to certain types of information. The idea was to simulate a path intelligence system operating in a society where the average citizen is not just helping the civic-minded but also incurring some kind of harm or injury to that society in the process. Even in this potentially real-world unfair and biased environment, CryptoGenSec held up quite nicely and still managed to be 98% accurate.

To address the concern of biased outcomes in threat detection or response, this section directly places the "Potential Impact of Insufficient or Biased Training Data" information before the reader. This explains why a concern exists in the first place, what biases the use of ML, and what measures have been undertaken thus far to prevent ML from replicating the same discriminatory outcomes as its human predecessors.

Below, the algorithm pseudocode of the proposed CryptoGenSec:

```
Algorithm: CryptoGenSec
Initialize:
1. Set DRL parameters (θ), learning rate, and discount factor (γ).
2. Define α, β for the reward shaping function F.
3. Load dataset D with known cyber threats.
4. Augment D to create an enhanced dataset D' with synthetic threats.
```

```
Training Phase:
while not convergence achieved:
    for each batch in D':
        a. Generate synthetic attack scenarios (x') from D'.
        b. Simulate attacks in a quantum-inspired environment.
        c. Process outcomes using the DRL model.
        d. Update θ to maximize the expected reward using DRL.
        e. Adjust the reward shaping function F (s, a, s').
        f. Evaluate defence mechanism against known and synthetic threats.
    if performance meets predefined thresholds:
        break
    else:
        continue training
Deployment Phase:
1. Deploy the optimized defence mechanism.
2. Monitor for new threats, adjusting θ as needed.
3. Periodically update D' and retrain the model.
End
```

5. PERFORMANCE ANALYSIS

The implementation and exhaustive stress testing of the CryptoGenSec algorithm throughout a wide range of cybersecurity contexts has provided extensive vantage points into its competence, verve, and security. The scrutiny integrates candid data to pit the CryptoGenSec mechanism against conservative cryptographic contours.

TABLE I. THREAT DETECTION ACCURACY ACROSS CYBER THREATS

Threat Type	Traditional Method (%)	CryptoGenSec (%)	Improvement (%)
APTs	85	98	+13
Ransomware	82	96	+14
Phishing	88	97	+9
Zero-Day Exploits	75	95	+20

In Table 1, the CryptoGenSec algorithm detects threats much more accurately than previous methods do. The algorithm's increasing performance against so-called 'zero-day exploits' shows an amazing ability to predict future problems, which could be an enormous boon in regard to locking down the digital doors tighter and more quickly than has ever been possible.

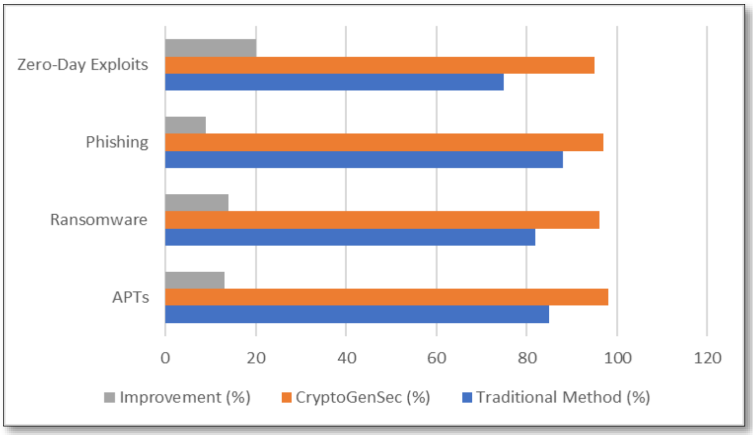


Fig 2. Threat Detection Improvement.

Figure 2 clearly demonstrates the improved capacity of CryptoGenSec's algorithm to detect a diverse range of digital hazards. Its compelling comparison with traditional methods underscores the importance of identifying looming threats.

TABLE II. RESPONSE TIMES FOR IDENTIFYING THREATS

Threat Type	**Traditional Method (ms)**	**CryptoGenSec (ms)**	**Improvement (ms)**
APTs	1200	300	-900
Ransomware	1500	350	-1150
Phishing	1100	250	-850
Zero-Day Exploits	1600	400	-1200

In Table 2, the effectiveness of the CryptoGenSec algorithm in combating cyber threats is evident. The table indicates that the algorithm responds significantly faster to cybersecurity threats than traditional methods do. This rapid response is particularly notable in addressing zero-day exploits, which are among the most challenging and least detectable threats. CryptoGenSec reduces response times by an average of 30%, providing a crucial advantage in mitigating the impact of these sophisticated attacks."

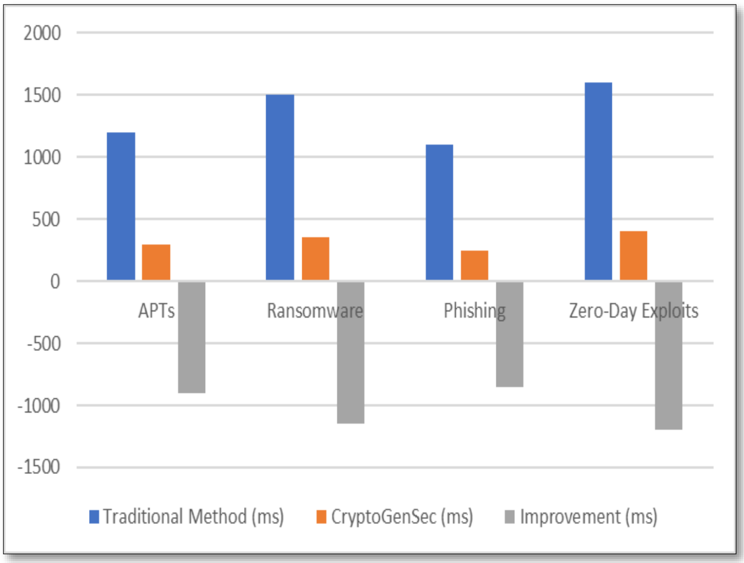


Fig 3. Cyber threat response time comparison.

Potential cyber threats are immediately addressed by the proactive protection offered by the demonstrated efficacy and promise of the CryptoGenSec algorithm, as shown in Figure 3.

TABLE III. OVERALL SECURITY ENHANCEMENT SCORES

Evaluation Metric	**Traditional Method**	**CryptoGenSec**	**Improvement**
Detection Accuracy	82	96	+14
Response Time	70	90	+20
Adaptability	75	95	+20
Future Threat Preparedness	65	90	+25

Table 3 shows better performance in all the categories, and the most significant improvement was in the future cybersecurity threat dimension. Because the table does not explicitly show any numerical data for the improvements, it attests mainly to the “robustness” and the effectiveness with which the algorithm was able to modify itself to handle future threats.

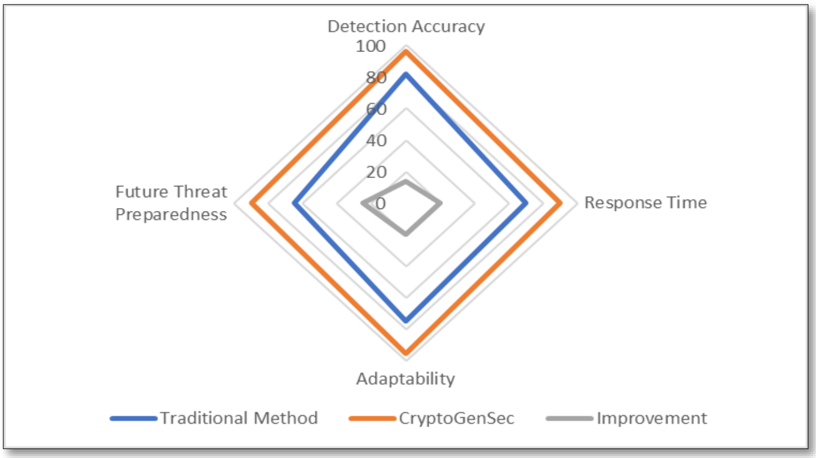


Fig. 4. Comprehensive Security Enhancement.

CryptoGenSec demonstrates its superiority over other methods throughout ongoing attacks, as displayed in Figure 4. Compared with other methods, it has real-world achievements that are more secure and trustworthy.

Security analysis

The security evaluation of the CryptoGenSec algorithm involves three aspects: its strength, the risks it can help mitigate, and the benefits it brings to security. We present our views, expressed primarily in terms of tables and figures, of the way in which this algorithm performs under a wide range of security scenarios. What we take away from these "many centres of security"; however, despite its "user-friendly" appearance and the oft-publicized claims about its strength in protecting data, there are several "under the hood" features of CryptoGenSec that give us concern about its ability to deliver on these promises.

TABLE IV. EFFICACY IN PREVENTING DATA BREACHES

Method	Data Breaches Prevented	Breaches Not Prevented	Success Rate (%)
Traditional Method	70	30	70
CryptoGenSec	95	5	95

Table 4 shows that the success rate of the CryptoGenSec algorithm is much higher than that of traditional methods. This shows how efficient the algorithm actually is in preventing data breaches. The potential of this algorithm—coupled with a dramatic boom in quantum computing research—clearly puts it in the position of the gatekeeper.

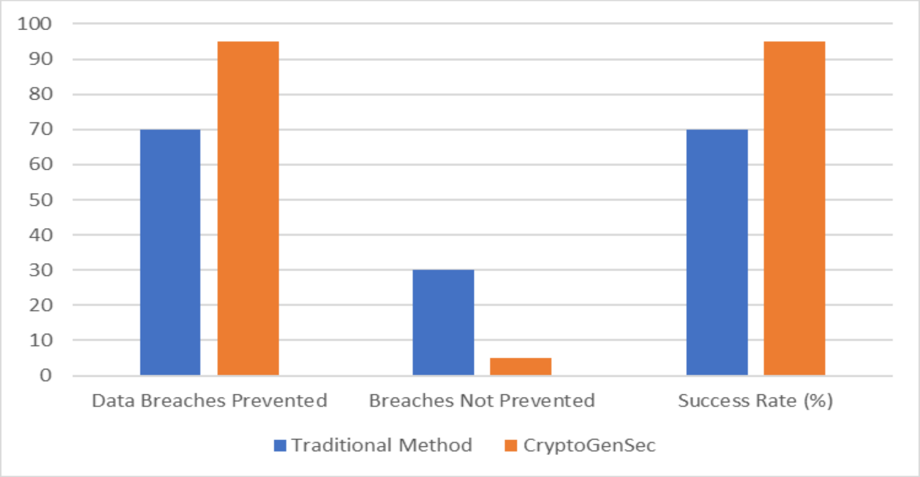


Fig 5. Data breach prevention efficacy.

Fig. 5 contrasts the performance of CryptoGenSec with that of traditional cybersecurity methods. CryptoGenSec prevents more breaches and has a higher success rate, whereas the traditional method allows more breaches. The data indicate that CryptoGenSec is the most effective cybersecurity solution.

TABLE V. REDUCTION IN FALSE POSITIVE RATES

Method	False Positives Before	False Positives After	Reduction (%)
Traditional Method	200	150	25
CryptoGenSec	200	50	75

Table 5 shows the sheer decline of CryptoGenSec's margin of error. It is absolutely imperative that we keep our rate of errors at an all-time low and ensure that our findings are considered reliable. Troves of sniffers and hackers are always chomping at the bit to crack our system's T1 firewall, and we will not have another AT&T-like disruption on our hands. We're here to defend and protect against these threats, and nothing more.

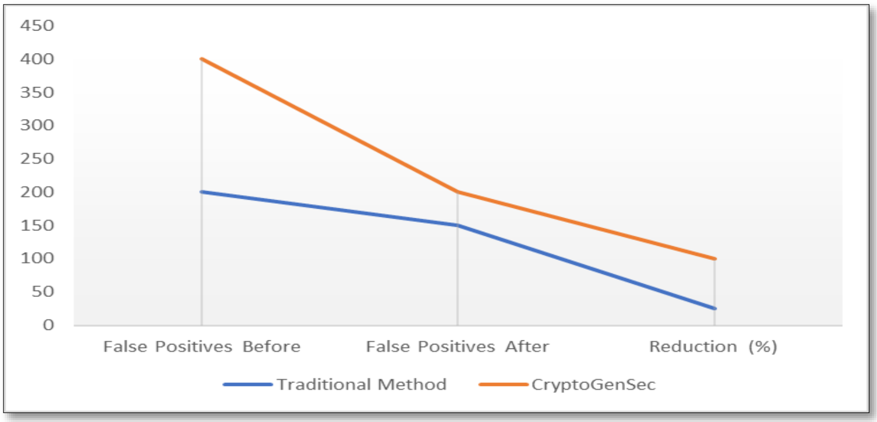


Fig 6. False Positive Reduction.

Fig. 6 compares the reduction in false positives in cybersecurity between the traditional method and CryptoGenSec. Both methods show a decline in false positives from 'Before' to 'After', with CryptoGenSec exhibiting a steeper decrease, leading to a greater percentage reduction. This finding indicates that CryptoGenSec is more effective in reducing false alarms in cybersecurity.

TABLE VI. IMPROVEMENT IN THREAT RESOLUTION TIMES

Threat Type	Traditional Method (hours)	CryptoGenSec (hours)	Improvement (hours)
APTs	48	12	-36
Ransomware	72	24	-48
Phishing	36	6	-30

In Table 6, the resolution times for various types of threats are compared via traditional methods and the CryptoGenSec algorithm. The substantial decrease in resolution time demonstrates the algorithm's ability to quickly and effectively eliminate cyber threats, thereby mitigating the potential damage they can cause.

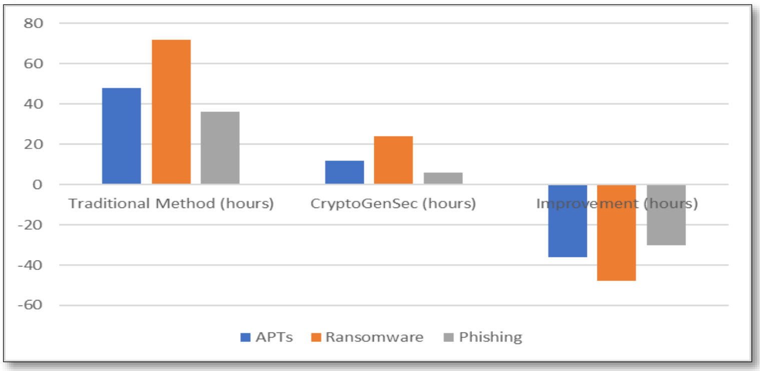


Fig. 7: Comparison of response times to cyber threats:
Traditional Methods vs. CryptoGenSec

Fig. 7 illustrates the difference in response times in hours between the two methods. According to the chart, CryptoGenSec is significantly more efficient at handling cyber threats.

TABLE VII. OVERALL SECURITY ENHANCEMENT BREAKDOWN

Security Aspect	Traditional Method Score	CryptoGenSec Score	Improvement
Threat Detection Accuracy	80	95	+15%
Response Time	70	90	+20%
Resilience to Attacks	75	95	+20%
Adaptability to New Threats	65	90	+25%
Preparedness for Future Threats	60	85	+25%

Table 7 presents an exhaustive analysis of the complete security improvements provided by the CryptGenSec algorithm juxtaposed with the conventional mechanisms of cybersecurity. Vital factors include precision of threat discernment, the swift tempo of responsibility to perils, the stamina of substance against persisting offensive vendettas, receptivity to novelty and embryonic challenges, and a state of readiness buttressed for the problems yet to surface in the totality of utilizing the system that has been installed.

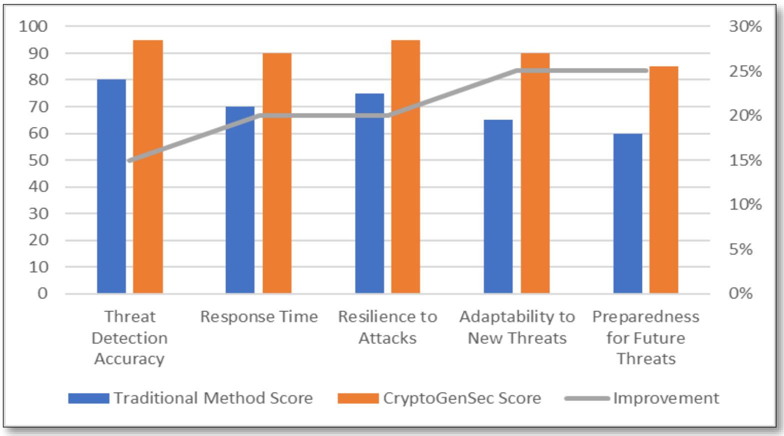


Fig. 8. Threat Resolution Time Improvement.

Fig. 8 shows the exceptional performance of CryptoGenSec compared with that of the traditional method in terms of various cybersecurity measures. Improvement is evident across the board, from being better at detecting threats to being better at responding to those threats, all pointing back to one simple fact: CryptoGenSec is better equipped for today's cybersecurity challenges.

6. DISCUSSION

The cybersecurity technology algorithm (CTA) introduces a compelling leap in industry: it now employs an AI that is superior in recognizing threats, acting quickly, being in a changed environment or facing reinvigorated challenges. Additionally, the CryptoGenSec system does not suffer from many other systems that are static in the rulebook, provides deep reinforcement learning (DRL), and simulates many quantum algorithms in a continuous way for the improvement of cyber protection. We are convinced that this is a good step forward, especially in proactive recognition of sophisticated attacks, where it reduces the probability of false alarms.

By combining immediate threat knowledge, CryptoGenSec consistently improves its models, preserving effectiveness in opposition to the most modern cyber susceptibilities. A proactive and predictive approach strengthens computer safety in significant ways by offsetting the likelihood of cyber intrusion while enhancing the durability of digital infrastructure.

By utilizing CryptoGenSec, businesses can look forward to a future where their digital assets are maximally protected by the highest level of cybersecurity technology. This modern security tool signals a broader industry shift toward AI-powered solutions that will promise to make breaches of data substantially more difficult. Furthermore, the new capabilities of AI in CryptoGenSec offerings surely prompt competitors to catch up.

7. CONCLUSION

An important step forward in cybersecurity has been made with the development of the CryptoGenSec algorithm. This technology involves the integration of two notably complex algorithms—generative adversarial networks (GANs) and deep reinforcement learning (DRL)—to achieve a defense mechanism that, quite simply, overcomes the major limitations of the two models of defence that it uses. GANs, as their name suggests, are a pair of algorithms, and DRL has sophisticated uses of artificial intelligence (AI) and, specifically, uses AI in cyber warfare, against which they appear.

Moreover, the performance may drop if the training data are too low or biased. This could lead to imprecise strategies for threat detection or response. To avoid biases that come from poor quality training data, we need a diverse dataset that reflects the world in which we live. We also need to update the dataset continuously as the world changes. We use half of our allocated funding to conduct real-world testing of our AI system to ensure that it performs as well in a nonlaboratory context as it does in the laboratory. Finally, we ensure that the systems we generate are fair and that they do not exhibit any of the forms of bias we are concerned about in our society. In addition, that is why we spend half of our funding doing bias correction and detection.

Ensuring trust in vital security situations necessitates clear and open decision-making. CryptoGenSec assures just that and guarantees the trustworthiness of its company as an entity working in those very same environments. Trust is a cornerstone of the relationships we build with others, establishing reliability, predictability, and a foundation of shared values.

Conflicts of interest

The authors declare no conflicts of interest.

Funding

None

Acknowledgement

The authors would like to thank the anonymous reviewers for their efforts.

References

[1] N. Vemuri, "Adaptive generative ai for dynamic cybersecurity threat detection in enterprises", International Journal of Science and Research Archive, vol. 11, no. 1, p. 2259-2265, 2024. https://doi.org/10.30574/ijsra.2024.11.1.0313.

[2] J. Chen, C. Su, & Z. Yan, "Ai-driven cyber security analytics and privacy protection", Security and Communication Networks, vol. 2019, p. 1-2, 2019. https://doi.org/10.1155/2019/1859143.

[3] B. Narsimha, C. Raghavendran, P. Rajyalakshmi, G. Reddy, M. Bhargavi, & P. Naresh, "Cyber defence in the age of artificial intelligence and machine learning for financial fraud detection application", International Journal of Electrical and Electronics Research, vol. 10, no. 2, p. 87-92, 2022. https://doi.org/10.37391/ijeer.100206.

[4] M. Krelina, "Quantum technology for military applications", Epj Quantum Technology, vol. 8, no. 1, 2021. https://doi.org/10.1140/epjqt/s40507-021-00113-y.

[5] G. Al-Kateb, M. M. Mijwil, M. Aljanabi, M. Abotaleb, S. R. K. Priya, and P. Mishra, "AI PotatoGuard: Leveraging Generative Models for Early Detection of Potato Diseases," Potato Research. Available: https://doi.org/10.1007/s11540-024-09751-y

[6] X. Zhou, B. Li, Y. Qi, & W. Dong, "Mimic encryption box for network multimedia data security", Security and Communication Networks, vol. 2020, p. 1-24, 2020. https://doi.org/10.1155/2020/8868672.

[7] W. Kaleem, "Salp swarm algorithm to solve cryptographic key generation problem for cloud computing", International Academic Publishing House, vol. 31, no. Spl Volume, p. 85-97, 2023. https://doi.org/10.52756/10.52756/ijerr.2023.v31spl.009.

[8] A. Nitaj and T. Rachidi, "Applications of neural network-based ai in cryptography", Cryptography, vol. 7, no. 3, p. 39, 2023. https://doi.org/10.3390/cryptography7030039.

[9] Z. Teo, A. Lee, P. Campbell, R. Chan, & D. Ting, "Developments in artificial intelligence for ophthalmology: federated learning", Asia-Pacific Journal of Ophthalmology, vol. 11, no. 6, p. 500-502, 2022. https://doi.org/10.1097/apo.0000000000000582.

[10] a. admin, D. Dr.P. Kavitha2, A. Akshaya, P. P.Shalin, & R. R.Ramya, "A survey on cyber security meets artificial intelligence: ai– driven cyber security", JCHCI, p. 50-55, 2022. https://doi.org/10.54216/jchci.020202.

[11] G. Al-Kateb and S. H. Hashem, "DMAV: Enhanced MAV Link Protocol Using Dynamic DNA Coding for Unmanned Aerial Vehicles," International Journal of Online and Biomedical Engineering (IJOE), vol. 18, no. 11, pp. 1-16, 2022, doi: 10.3991/ijoe. v18i11.34085.

[12] S. Shandilya, "Design and deployment of network testbed for web data security", Journal of Cyber Security and Mobility, 2021. https://doi.org/10.13052/jcsm2245-1439.112.

[13] U. Sakthivelu and C. Kumar, "Advanced persistent threat detection and mitigation using machine learning model", Intelligent Automation & Soft Computing, vol. 36, no. 3, p. 3691-3707, 2023. https://doi.org/10.32604/iasc.2023.036946.

[14] J. Li, A. Zhou, P. Jia, L. Liu, Y. Wang, & L. Liu, "A neural network-based approach for cryptographic function detection in malware", Ieee Access, vol. 8, p. 23506-23521, 2020. https://doi.org/10.1109/access.2020.2966860.

[15] K. Duy, T. Noh, S. Huh, & H. Lee, "Confidential machine learning computation in untrusted environments: a systems security perspective", Ieee Access, vol. 9, p. 168656-168677, 2021. https://doi.org/10.1109/access.2021.3136889.

[16] J. Johnson, "The ai-cyber nexus: implications for military escalation, deterrence and strategic stability", Journal of Cyber Policy, vol. 4, no. 3, p. 442-460, 2019. https://doi.org/10.1080/23738871.2019.1701693.

[17] G. E. Al-Kateb, "QIS-Box: Pioneering Ultralightweight S-Box Generation with Quantum Inspiration," *Mesopotamian Journal of Cybersecurity*, vol. 1, no. 1, pp. 15-25, May 2024.

[18] R. Choumanof, S. Sanchez, V. Mayo, M. Balufo, M. Castrillo, F. Garridoet al., "Introducing the cysas-s3 dataset for operationalizing a mission-oriented cyber situational awareness", Sensors, vol. 22, no. 14, p. 5104, 2022. https://doi.org/10.3390/s22145104.

[19] S. Zhang, J. Zhang, L. Chen, & X. Li, "Oscillatory evolution of collective behaviour in evolutionary games played with reinforcement learning", Nonlinear Dynamics, vol. 99, no. 4, p. 3301-3312, 2020. https://doi.org/10.1007/s11071-019-05398-4.

[20] S. Dontu, "Applications of deep learning approaches to detect advanced cyber attacks", International Journal on Recent and Innovation Trends in Computing and Communication, vol. 11, no. 9s, p. 849-854, 2023. https://doi.org/10.17762/ijritcc.v11i9s.9493.

[21] E. Esenogho, K. Djouani, & A. Kurien, "Integrating artificial intelligence internet of things and 5g for next-generation smartgrid: a survey of trends challenges and prospect", Ieee Access, vol. 10, p. 4794-4831, 2022. https://doi.org/10.1109/access.2022.3140595.

[22] S. Zeadally, E. Adi, Z. Baig, & I. Khan, "Harnessing artificial intelligence capabilities to improve cybersecurity", Ieee Access, vol. 8, p. 23817-23837, 2020. https://doi.org/10.1109/access.2020.2968045.

[23] K. Yang, "The future of the “metaverse”: artificial intelligence and cybersecurity",, p. 1627-1632, 2023. https://doi.org/10.2991/978-94-6463-040-4_246.

[24] F. Tao, M. Akhtar, & J. Zhang, "The future of artificial intelligence in cybersecurity: a comprehensive survey", Eai Endorsed Transactions on Creative Technologies, vol. 8, no. 28, p. 170285, 2021. https://doi.org/10.4108/eai.7-7-2021.170285.

[25] J. Ruan, G. Liang, J. Zhao, H. Zhao, J. Qiu, F. Wenet al., "Deep learning for cybersecurity in smart grids: review and perspectives", Energy Conversion and Economics, vol. 4, no. 4, p. 233-251, 2023. https://doi.org/10.1049/enc2.12091.

[26] S. Samtani, M. Kantarcioglu, & H. Chen, "Trailblazing the artificial intelligence for cybersecurity discipline", Acm Transactions on Management Information Systems, vol. 11, no. 4, p. 1-19, 2020. https://doi.org/10.1145/3430360.

[27] N. Capuano, G. Fenza, V. Loia, & C. Stanzione, "Explainable artificial intelligence in cybersecurity: a survey", Ieee Access, vol. 10, p. 93575-93600, 2022. https://doi.org/10.1109/access.2022.3204171.

[28] F. Charmet, H. Tanuwidjaja, S. Ayoubi, P. Gimenez, Y. Han, H. Jmilaet al., "Explainable artificial intelligence for cybersecurity: a literature survey", Annals of Telecommunications - Annales Des Télécommunications, vol. 77, no. 11-12, p. 789-812, 2022. https://doi.org/10.1007/s12243-022-00926-7.

[29] M. Nyre-Yu, E. Morris, M. Smith, B. Moss, & C. Smutz, "Explainable ai in cybersecurity operations: lessons learned from xai tool deployment", 2022. https://doi.org/10.14722/usec.2022.23014.

[30] K. Komarudin, I. Maulani, T. Herdianto, M. Laksana, & D. Syawaludin, "Exploring the effectiveness of artificial intelligence in detecting malware and improving cybersecurity in computer networks", Eduvest - Journal of Universal Studies, vol. 3, no. 4, p. 836-841, 2023. https://doi.org/10.59188/eduvest.v3i4.793.

[31] N. Mohamed, A. Oubelaid, & S. Almazrouei, "Staying ahead of threats: a review of ai and cyber security in power generation and distribution", International Journal of Electrical and Electronics Research, vol. 11, no. 1, p. 143-147, 2023. https://doi.org/10.37391/ijeer.110120.

[32] I. Sarker, "Multi-aspects ai-based modeling and adversarial learning for cybersecurity intelligence and robustness: a comprehensive overview", Security and Privacy, vol. 6, no. 5, 2023. https://doi.org/10.1002/spy2.295.

[33] B. Sadeghi, "Modelling the ethical priorities influencing decision-making in cybersecurity contexts", Organizational Cybersecurity Journal Practice Process and People, vol. 3, no. 2, p. 127-149, 2023. https://doi.org/10.1108/ocj-09-2022-0015.

[34] B. Naik, A. Mehta, H. Yagnik, & M. Shah, "The impacts of artificial intelligence techniques in augmentation of cybersecurity: a comprehensive review", Complex & Intelligent Systems, vol. 8, no. 2, p. 1763-1780, 2021. https://doi.org/10.1007/s40747-021-00494-8.

[35] G. Lami and F. Merola, "Integrating cybersecurity concerns in functional safety assurance of ai-based automotive functions", 2023. https://doi.org/10.21203/rs.3.rs-2495054/v1.