WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Application of AI in Cryptography

Harsh Kathe[1],Dr. Harshali Patil[2]

[1]Department of Information Technology and Computer Science, S K Somaiya College, Somaiya Vidyavihar University, Mumbai, India
harsh.kathe@somaiya.edu
[2]Department of Information Technology and Computer Science, S K Somaiya College, Somaiya Vidyavihar University, Mumbai, India
harshali.yp@somaiya.edu

ABSTRACT :

Artificial intelligence (AI) is a modern technology that allows many advantages in daily life, such as predicting the weather, finding directions, classifying images and videos, and even automatically generating code, text, and videos(Nitaj & Rachidi, 2023). Cryptography is defined as the analysis of encryption or secretive writing of information using mathematical & logical concepts to prevent data from being compromised(Sumathi et al., 2023). This paper covers the study of the overall application of Artificial Intelligence in Cryptography including the latest applications.

1 Introduction :

Encryption is the process by which data is secured from unauthorized access, only those with authorized public or private keys can have access to the data. Even though today's encryption techniques are virtually impregnable, encrypted communications may sometimes be broken via cryptanalysis, also known as code-breaking(Kapoor et al., 2016). The rapid growth of digital communication has increased the need for digital security, which can be accomplished through cryptography.

The term Artificial Intelligence (AI) covers a range of methodologies and applications that are designed to enable a computer to undertake tasks that are conventionally the domain of human intelligence(Nitaj & Rachidi, 2023). The current applications of AI range from speech recognition finance, avionics, navigation, gaming, robotics medicine, etc. This paper gives an overview of such applications focusing on cryptography while referencing more technically oriented papers that are relevant to the material.(Blackledge & Mosola, 2020)

2 Literature Review :

Jonathan Blackledge and Napo Mosola (2020) described the different applications of AI in cryptography. This paper also covers the latest applications of AI in cryptography like AI-Driven Cryptographic Algorithm Optimization, AI in Quantum Cryptography, Privacy-Preserving AI, and AI-Enhanced Security Protocols.

Sumathi M S (2023) discussed the application of AI with hybrid cryptography based on the survey they took, displaying that cryptographic methods are used to protect the data throughout the data exchange process and during different interactions. These methods are commonly used these days which makes them insecure. An innovative hybrid cryptographic approach for enhancing data security throughout network transmission is presented in this article. This paper also covers the problems faced in the application of AI in cryptography.

Mengting Liu (2023) discussed the application of image sharing and encryption based on visual cryptography in NSAI (Networking Systems of AI) and gave the methods and steps of shared image preprocessing in detail, which will also be discussed further in this paper.

3 Problem Statement :

There are many applications of artificial intelligence in cryptography that have been addressed in previous research papers which are used as references in this paper. All these papers were accurate with no research gaps, but the IT world faces new problems every year that require solutions with unique approaches. In terms of cryptography, it must be flexible with the latest technologies to make digital communication more secure.

If cryptography doesn’t adapt according to the new technologies and innovations digital communication can't stay secure because eventually it will be outdated and secret keys and encryptions will be familiar and easy to crack. With the growth of Artificial Intelligence, it's more important than ever to be up-to-date in case of confidential communication and processes.

4 Research Objective :

As discussed in 'Problem Statement' the previous research papers have covered appropriate points. The latest technologies related to the application of AI must be considered and that's what is included in this paper.
This paper covers the latest application of AI in cryptography like AI-Driven Cryptographic Algorithm Optimization, AI in Quantum Cryptography, AI for Cryptanalysis, Privacy-Preserving AI, and AI-Enhanced Security Protocols.
This paper will also define the technologies related to AI that may be applied in cryptography and may be threatening to digital communication.

5 Research Methods :

A. Literature Review: Conducted a comprehensive review of existing literature on AI and cryptography to gain a thorough understanding of the current state of research in this area. I have studied the latest developments and applications to identify any research gaps. I used tools such as,

- connectedpaper.com
- scispace.com
- chatpdf.com

to find relevant literature and identify research gaps in this field.

B. Empirical Research: Experiments are conducted and studies are performed to demonstrate the effectiveness of AI in cryptography, such as evaluating AI-driven cryptographic algorithm optimization, analyzing the use of AI in quantum cryptography, or assessing the performance of AI for cryptanalysis.

C. Case Studies: Analyzing and presenting case studies of real-world applications of AI in cryptography to showcase its practical relevance and impact.

D. Comparative Analysis: Different AI-based cryptographic approaches and methodologies are compared to evaluate their strengths, limitations, and potential implications for digital security.

6 Research Findings :

A. AI-Driven Cryptographic Algorithm Optimization:

AI optimization algorithms play a crucial role in various domains like:

- Resource Allocation
- Data Analysis
- Engineering and Design
- Healthcare

AI optimization algorithms are the essence of intelligent decision-making, enabling efficient problem-solving. Drawing inspiration from nature and mathematics, these algorithms offer versatile tools for addressing optimization problems, contributing to a smarter and more efficient world. As technology advances, its impact on shaping our future will surely grow ai (*AI Optimization Algorithms: The Brains Behind Intelligent Decision-Making | by Alya Rahik | Medium*, n.d.).

Types of AI Optimization Algorithms:

- Genetic Algorithms (GA)
- Particle Swarm Optimization (PSO)
- Simulated Annealing
- Ant Colony Optimization (ACO)
- Gradient Descent

AI optimization algorithms are the brains behind intelligent decision-making, enabling businesses and researchers to tackle complex problems with efficiency and precision.
It follows a general procedure:

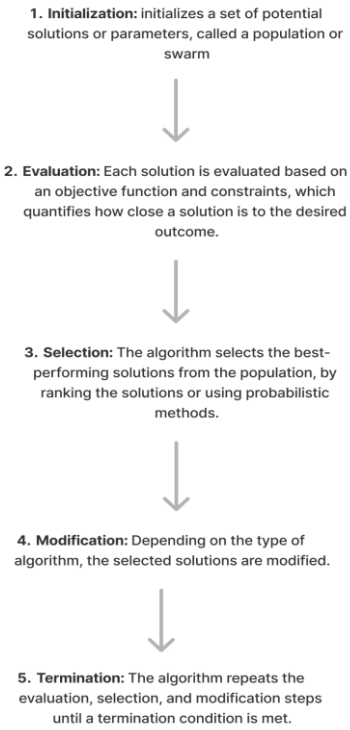


Fig.1 General procedure of AI-driven cryptographic algorithm(*Welcome to FigJam – FigJam*, n.d.).

B. AI in Quantum Cryptography:

Quantum cryptography is an advanced sub-field of cryptography based on the principles of quantum mechanics to ensure secure communication. Unlike classical cryptography, which typically utilises complex mathematical algorithms to encode data, quantum cryptography uses the physical properties of quantum particles, such as photons, to create a secure communication system. Quantum key distribution (QKD) is a secure method that utilises quantum mechanics concepts to create and distribute cryptographic keys between two parties(Radanliev, 2024).

Fig.2 Procedure of AsI in Quantum Cryptography (Online AI Flowchart Generator —— 7-Day Unlimited Use for New Users, n.d.).

C. Privacy-Preserving AI:

Today we can use artificial intelligence for many things from unlocking an iPhone to detecting diseases in their early stages and translating languages automatically. AI helps us in various fields, these AI systems are often built on Machine Learning. These systems are based on sensitive and private data. A technique was required to use AI technology while preserving the privacy of the data used in them. Privacy-Preserving AI

Key Benefits of Privacy-Preserving AI:

- **Data Protection**: Safeguards sensitive personal information from exposure.
- **Customer Trust**: Prioritizing privacy builds customer loyalty and confidence.
- **Regulatory Compliance**: Helps organizations meet data privacy laws like GDPR and CCPA.
- **Reputation Preservation**: Reduces risks of data breaches and associated reputational damage.

Technique	Description
Differential Privacy	Adds controlled noise to data, ensuring outputs don't reveal individual information
Homomorphic Encryption	Performs computations on encrypted data without decrypting
Secure Multi-Party Computation	Enables collaborative computations without revealing individual inputs
Federated Learning	Trains models on decentralized data without centralization
Hybrid Approaches	Combines multiple techniques to leverage their strengths

Fig3.Core Privacy-Preserving Techniques (Palle & Kathala, 2024)

Advantages	Disadvantages
Strong privacy guarantees, quantifies privacy loss	May reduce data utility, computationally expensive
Ensures data confidentiality, high security	Significant computational overhead, efficiency challenges
Protects privacy in distributed settings	Computationally intensive, scalability limitations
Sensitive data never leaves device, useful for distributed data	Potential communication overhead
Stronger privacy guarantees, better utility trade-offs	Increased complexity, careful design required

Fig4.Advantages and Disadvantages of Privacy-Preserving AI (Palle & Ka[]thala, 2024)

D. AI-Enhanced Security Protocols:

AI is drastically changing the field of cybersecurity by providing powerful tools for detecting and preventing cyber threats, safeguarding sensitive and private data, and overall enhancement of security.

It can analyze vast data sets, identify potential threats and develop new algorithms to detect and prevent novel attacks on your digital assets. It can encrypt sensitive data, monitor access, and identify unauthorized users, strengthening data protection and challenging data access for unauthorised users (*Enhancing Cyber Security Measures by Integrating AI Systems*, n.d.).

Some Protocols are:

1. Secure Multiparty Computation (SMPC)-

Secure multiparty computation (MPC / SMPC) is a cryptographic protocol that distributes computation across multiple parties where no individual party can see the other parties' data. It can enable data scientists and analysts to compliantly, securely, and privately compute on distributed data without ever exposing or moving it (Sowmya & Mary Anita, 2023).

Eg.

Let's assume three coworkers - A, B, and C - want to calculate their average salary without revealing their individual salary information to each other. They can use secure multiparty computation, in this case, to compute the average of their salaries without sharing individual salaries.

How will It work?

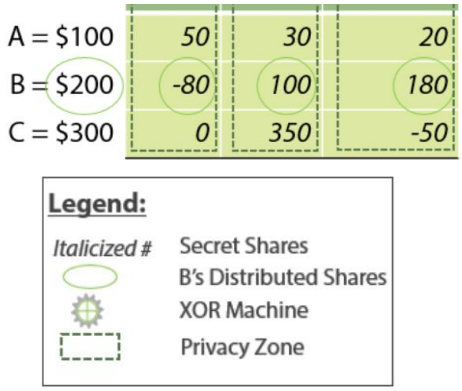


Fig5.(What Is Secure Multiparty Computation? - SMPC/MPC Explained | Inpher, n.d.)

Here, the salary of A i.e. $100 in additive secret sharing, $100k is split into three randomly generated pieces: $20k, $30k, and $50k for example. A keeps one of these secret shares ($50k) for himself and distributes one secret share to B ($30k) and C ($20k). B and C also secret-share their salaries while following the same process(*What Is Secure Multiparty Computation? - SMPC/MPC Explained | Inpher*, n.d.).

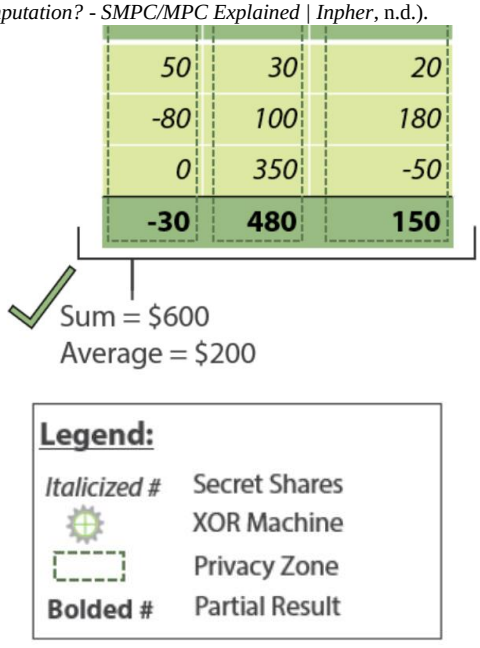


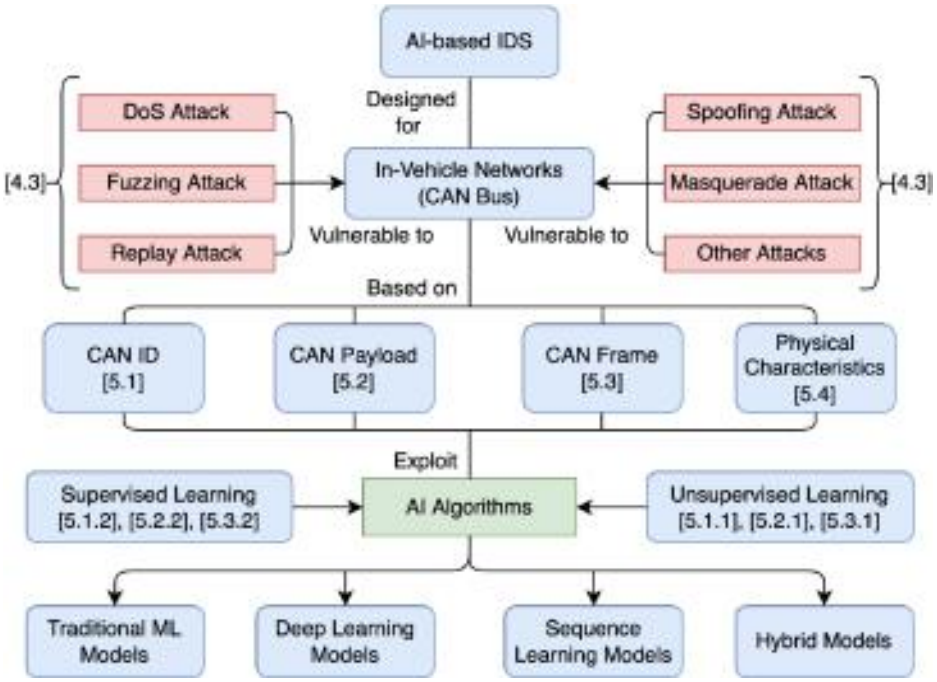
Fig 6.(What Is Secure Multiparty Computation? - SMPC/MPC Explained | Inpher, n.d.)

Now if they calculate the average of received secret shares including their secret share they will be able to calculate the average of their salaries without sharing their salary.

2. AI for Intrusion Detection-

Protecting the cloud and the network is an important duty performed by Intrusion Detection Systems in cybersecurity. Initially, it required humans to observe and identify intrusions, which proved to be an inefficient method.

Cybersecurity experts have realized that the increased use of cloud computing has created a greater need for IDS to identify possible breaches, ensure safety, and find effective ways to detect attacks.
While there were several security measures in place, none could identify threats amidst dense cloud and network traffic. These limitations are addressed by the development of AI-based IDS for quick and effective analysis of attacks.
Some AI-based Intrusion Detection Systems:



7 Conclusion and Future Work :

AI in cryptography is a rapidly expanding field with new applications being developed every day. This paper discusses some of the significant applications in this field, drawing from previous research papers and the latest advancements. It does not include any questionnaires or surveys.

The research findings provide insight into the current use of AI in the fields of cybersecurity and cryptography Although the research covers the latest AI applications in cryptography and cybersecurity, it does not encompass future applications or updates in current technologies.

This research serves as a foundational understanding of past applications and their functionalities, highlighting any missing applications that future researchers should consider adding.

8 REFERENCES :

1. *AI Optimization Algorithms: The Brains Behind Intelligent Decision-Making | by Alya Rahik | Medium*. (n.d.). Retrieved October 13, 2024, from https://medium.com/@alyarahik/ai-optimization-algorithms-the-brains-behind-intelligent-decision-making-f32f1c5c48de
2. Blackledge, J., & Mosola, N. (2020). Applications of Artificial Intelligence to Cryptography. *Transactions on Machine Learning and Artificial Intelligence*, *8*(3), 21–60. https://doi.org/10.14738/tmlai.83.8219
3. *Enhancing Cyber Security Measures by Integrating AI Systems*. (n.d.). Retrieved October 13, 2024, from https://kahedu.edu.in/enhancing-cyber-security-measures-by-integrating-ai-systems/
4. Kapoor, V., Kapoor, V., & Yadav, R. (2016). A Hybrid Cryptography Technique for Improving Network Security. *Article in International Journal of Computer Applications*, *141*(11), 975–8887. https://doi.org/10.5120/ijca2016909863
5. Nitaj, A., & Rachidi, T. (2023). Applications of Neural Network-Based AI in Cryptography. *Cryptography 2023, Vol. 7, Page 39*, *7*(3), 39. https://doi.org/10.3390/CRYPTOGRAPHY7030039
6. *Online AI Flowchart Generator —— 7-day Unlimited Use for New Users*. (n.d.). Retrieved October 13, 2024, from https://www.edraw.ai/feature/flowchart-maker.html?channel=google_adonline&utm_source=google&utm_medium=cpc&utm_campaign=google_adonline&utm_term=google-ads?slug=edraw.ai-ex-en-ppc&m_pid=20032&gad_source=1&gclid=CjwKCAjwvKi4BhABEiwAH2gcw7HysgPmjr22bc1Sv6tbaSvJOtCeiIB6VSZyWKVbpdwzTBzeIOSSrRoC7asQAvD_BwE
7. Palle, R. R., & Kathala, K. C. R. (2024). Privacy-Preserving AI Techniques. *Privacy in the Age of Innovation*, 47–61. https://doi.org/10.1007/979-8-8688-0461-8_5

8. Radanliev, P. (2024). Artificial intelligence and quantum cryptography. In *Journal of Analytical Science and Technology* (Vol. 15, Issue 1). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1186/s40543-024-00416-6
9. Sowmya, T., & Mary Anita, E. A. (2023). A comprehensive review of AI based intrusion detection system. *Measurement: Sensors*, *28*, 100827. https://doi.org/10.1016/J.MEASEN.2023.100827
10. Sumathi, M. S., Shruthi, J., Jain, V., Kumar, G. K., & Khan, Z. Z. (2023). Using Artificial Intelligence (AI) and Internet of Things (IoT) for Improving Network Security by Hybrid Cryptography Approach. *Evergreen*, *10*(2), 1133–1139. https://doi.org/10.5109/6793674
11. *Welcome to FigJam – FigJam*. (n.d.). Retrieved October 13, 2024, from https://www.figma.com/board/FBn1foRpZImyBr5g86PrAL/Welcome-to-FigJam?node-id=0-1&node-type=canvas&t=2pL7DcSe5UPjSMKr-0
12. *What is Secure Multiparty Computation? - SMPC/MPC Explained | Inpher*. (n.d.). Retrieved October 13, 2024, from https://inpher.io/technology/what-is-secure-multiparty-computation/