


Chapter 4

An Adaptive Cryptography Using OpenAI API: Dynamic Key Management Using Self Learning AI

R. Valarmathi

 <https://orcid.org/0000-0002-1535-4552>

Sri Sairam Engineering College, India

R. Uma

 <https://orcid.org/0000-0002-0053-0162>

Sri Sairam Engineering College, India

P. Ramkumar

Sri Sairam College of Engineering, India

Srivatsan Venkatesh

Sri Sairam Engineering College, India

ABSTRACT

Security functions which are present now, such as the SHA series of hash functions, other brute force prevention protocols, and much more, are keeping our cyber fields safe from any script-kiddies and professional hackers. But the recent study shows that penetration tools are optimised in numerous ways, enabling the hackers to take in a big advantage over our key logging and brute forcing prevention tactics, allowing them to make a clean hit over the fragile databases. Many of the existing domains now are optimised with the added benefit of artificial intelligence support. Specifically, the OpenAI API market has grown plentiful of their uses, and the password hash automation now has a time to get upgraded.

DOI: 10.4018/979-8-3693-1642-9.ch004

1. INTRODUCTION

The Idea is to create a self-learning and bug withstanding AI. A tremendous data is fed and worst case history of bugs and hackers are collected, using the trustworthy OpenAI's API. Their algorithm is used to train and get the response of a threat immediately instead of a 24hr monitoring of status of the medium. The AI will replace few tedious tasks, making sure to give a complete log of an error or a breach. It locks the important databases and other codes from getting spread, into completely removing any bugs if the bugs which are in active attacking module that has previously encountered by some other instance of this same AI. Moreover, this AI can also be used to shift few keys in the current encryption status, creating new keys over the user location, as well as the domain location systems. This is the future of the great vault of security and privacy.

OpenAI Models are easier to retrieve and train, due to its increasing popularity and their dataset training methods. The dynamic key encryption requires predictive hash generation as well as key storage by AI. The AI model that we are about to train and analyse is the slight variation of OpenAI's API, specifically GPT-3 language model for NLP. First is the analysis phase, in which the data is collected from previously faulty dataset of cryptographic environments, security incidents and its respective cyber protection, the ways of bypassing the history of cyber malfunctions and data breaches, anomalies in existing system, and all the other defects within a system, and finds preventive measures. This form of data collection is especially useful when providing and feeding it to an OpenAI API connected Cryptography machine. It finds the error, if the symptoms of the attack are related to any previous known attack strategy, or if it encounters a new kind of attack, it must store the attack pattern in its database, and must adapt to the upcoming attack by another form of defence, dynamic key management.

Dynamic key Management ensures that the key of certain hash or information gets randomised multiple times in our systems, servers as well as host systems. Dynamic key Management AI also must be responsible for storage, delivery and generating new forms of key hash, either by random generation, or by seeded noise generation. When using a seeded noise generated key, it is a good practice to choose the seed of randomised noise with another randomizer with a unique seed, which ensures that even the seed of the current key gets blown; the decisive algorithm changes the seed of the randomizer responsible for changing seeds of key randomizer. And thus, a triple layer key protection as well as Dynamic key handling is done by OpenAI tool. This Layered Security in any form of media is fool proof and easily operable to an admin as well. Thus the next security encryption comes in the format of protection of this AI from a hack-insider or key logger for API of AI.

Together with all these qualities, we are going to create an AI capable of detection of all forms of intrusion

2. BACKGROUND

Cybersecurity is the most required field of division in this modern era, which solely runs on the digital media for data transfer and usage. In this day and age, thieves may not require your wallet to get your identification, but may readily steal it from the systems you are trusting. This unfolds the term "cyber-crime". Traditional security measures face challenges due to evolving hacking techniques, including the use of script bots and AIs (Pearce et al., 2023), rendering manual penetration avoidance and security measures less effective.

18 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/an-adaptive-cryptography-using-openai-api/340973

Related Content

A Pairing-based Homomorphic Encryption Scheme for Multi-User Settings

Zhang Wei (2020). *Cryptography: Breakthroughs in Research and Practice* (pp. 295-305).

www.irma-international.org/chapter/a-pairing-based-homomorphic-encryption-scheme-for-multi-user-settings/244920

Efficient Energy Saving Cryptographic Techniques with Software Solution in Wireless Network

Alka Prasad Sawlikar, Zafar Jawed Khan and Sudhir Gangadhar Rao Akojwar (2020). *Cryptography: Breakthroughs in Research and Practice* (pp. 159-179).

www.irma-international.org/chapter/efficient-energy-saving-cryptographic-techniques-with-software-solution-in-wireless-network/244912

Security Issues and Countermeasures of Online Transaction in E-Commerce

Sarvesh Tanwar Harshita and Sarvesh Tanwar (2016). *Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security* (pp. 273-302).

www.irma-international.org/chapter/security-issues-countermeasures-online-transaction/153080

A Software Library for Multi Precision Arithmetic

Kannan Balasubramanian and Ahmed Mahmoud Abbas (2018). *Algorithmic Strategies for Solving Complex Problems in Cryptography* (pp. 195-227).

www.irma-international.org/chapter/a-software-library-for-multi-precision-arithmetic/188524

Fundamentals of Quantum Computing, Quantum Supremacy, and Quantum Machine Learning

Kamaljit I. Lakhtaria and Vrunda Gadesha (2021). *Limitations and Future Applications of Quantum Cryptography* (pp. 21-46).

www.irma-international.org/chapter/fundamentals-of-quantum-computing-quantum-supremacy-and-quantum-machine-learning/272363