(IJRST) 2020, Vol. No. 10, Issue No. III, Jul-Sep **e-ISSN: 2249-0604, p-ISSN: 2454-180X**

A Research on Cyber Security and Artificial Intelligence[1]

Anirudh Dahiya

DOI: 10.37648/ijrst.v10i03.001

Received: 02nd July, 2020; Accepted: 30th July, 2020; Published: 27th August, 2020

ABSTRACT

Nowadays cyberattack is very common and also very dangerous. It not only corrupts data but also steals money from the user's accounts. To prevent this, we introduce CSAAI. Artificial intelligence is based on machine, that means there is no involvement of humans. In computers, AI itself is defined as intelligent agents. A device that uses its own environment and takes a decision on behalf of humans and enhances its result. Colloquially, the expression "man-made reasoning" is applied when a machine impersonates "subjective" capacities that people partner with other human personalities, for example, "learning" and "critical thinking".

1. INTRODUCTION

In Cybersecurity, data is being protected from network attacks, computers attack from ransomware, and unauthorized access. In a computing context, security incorporates both cybersecurity and physical security. In 2017, the danger level to big business IT keeps on being at exceptionally elevated levels, with day by day accounts in the media of huge breaks and assaults [3], for example, qualification reuse, Session Hijacking and Man in Middle Attack, DDOS Attack, XSS, SQL infusion, Phishing, Malware, Password Hijacking, IP satirizing, DNS ridiculing, SMURF assault, junk mail, Frolic assault, Replay assault, Traffic Analysis. In this way, so as to keep from such sort of digital assaults we require solid cybersecurity. Components of cybersecurity [4] incorporate Application Security, Information security, Network Security, Disaster recuperation/business progression arranging, End-client instruction. These days Information Security is given the assistance of encryption and unscrambling strategies, for example, AES, DES,2 DES, Triple DES, Serpent, Two-fish, Blowfish, IDE and Authentication procedures, for example, Digital marks, MD5, SHA1, and so on calculations. The Network Security is given by means of utilizing IPV6 web convention security (IPSEC) layer. There is vast scope in which cyber-attack is plaguing clients, organizations, and even nations. The Wanna Cry ransomware assault scrambled clients' information and requested payoff instalments in return for returning access to the information [1]. Dyn, an organization that runs the Internet area name framework for some, driving locales, was the survivor of a dispersed refusal of-administration (DDoS) assault, bringing about enormous pieces of the Internet getting out of reach. Also, the ongoing Petya digital damage assault seems, by all accounts, to be aimed at frameworks in Ukraine however has spread to different nations. Programming regularly meets useful prerequisites for buyer use yet neglects to work in security assurances, prompting bargains and expansive unintended results. Worked in versus Bolted on Much has been expounded on the effect of unreliable programming for regular shoppers. For instance, lacking security assurances have prompted the "insidious evaluation" class of assaults against unreliable programming fixing systems, empowering the disease and weaponization of a huge number of regular gadgets. These gadgets, for example, webcams and DVRs, would then be able to be sent in assaults like the DDoS

[1] *How to cite the article:* Dahiya A., A Research in Cyber Security and Artificial Intelligence, IJRST, Jul-Sep 2020, Vol 10, Issue 3, 1-5, DOI: http://doi.org/10.37648/ijrst.v10i03.001

against Dyn. In spite of the fact that there are numerous features of these occurrences, assaults like these feature the need to move to make sure about the framework and programming plan and usage that manufacture unseemly security insurances from the earliest starting point. The conventional programming advancement lifecycle (SDLC) has frequently tended to security worries in the testing stage, which brings about extravagant fixes6 or, more awful, security gives that aren't revealed until activity. Secure improvement rehearses incorporate security-related exercises in each period of the SDLC, yielding advantages by making security a consistent concern as opposed to just a piece of test techniques. Numerous associations including Microsoft (www.microsoft.com/en-us/dl), NIST, and the Open Web Application Security Project (www.owasp.org/index.php/OWASP_Secure_Software_Development_Lifecycle_Project) offer secure SDLC models, and numerous advances have been made in secure coding practices, for example, entrance testing, secure code instruments, and analysers, and endeavour relief methods [2]. However, this security progresses to risk being underutilized. For security advances to be "inherent" from the earliest starting point, as opposed to "darted on" toward the end, security specialists must work with industry experts to get familiar with the difficulties of security in the designing channels and to manufacture associations that develop and progress developments from research to rehearse. Regardless of secure SDLC models and advances in secure improvement methods, there are many open regions of research. Further, there's a hole between secure improvement look into and secure advancement rehearses that must be tended to with both network building and new developments.

A. Cyber Attack Types [6]: -

- 2007 cyber-attacks on Estonia, wide-ranging attack targeting government and commercial institutions
- 2010 cyber-attacks on Burma, related to the 2010 Burmese general election.
- 2010 Japan–South Korea cyber warfare.
- 2013 Singapore cyber-attacks, attack by Anonymous "in response to web censorship regulations in the country, specifically on news outlets".
- #OpIsrael, a broad "anti-Israel" attacks. Cyber-attacks during the Russo-Georgian War.
- July 2009 cyber-attacks, against South Korea and the United States.
- Operation Olympic Games, against Iranian nuclear facilities, allegedly conducted by the United States.

B. Importance Of AI in Cyber Security: - [2]

- The best approach to effective cyber security is to identify the threats, vulnerabilities and risks the organization faces, and to forecast the impact and likelihood of such risks materializing but some of the mistakes can also be done in such a procedure by cyber security creature.
- Moreover, this is time consuming.
- Moreover, this procedure of human finding the vulnerabilities, threats, Prevention technique and Implementation is not so appropriate and no. of mistakes can be done by the security person providing security.
- Intelligent robots can be used to make chances of error almost nil and greater precision and accuracy is achieved.
- Artificial intelligence can be utilized in carrying out repetitive and time-consuming tasks efficiently and dangerous tasks execution. They do not require sleep or breaks, and are able to function without stopping.

II. RELATED WORK

To fight with Cyber Security Big Data, Cloud Computing, IOT and AI can be used,

Following are the steps:

1) Log in:

In the wake of getting sign-in client will get to a window and machine gave by man-made consciousness will take a choice whether a client who has signed into the site is a legitimate or un-proposed client and to obstruct its entrance naturally with no human order and impedance. In the event that client is unintended, at that point access to that client will be denied and if that individual is a typical client than that client is ensured.

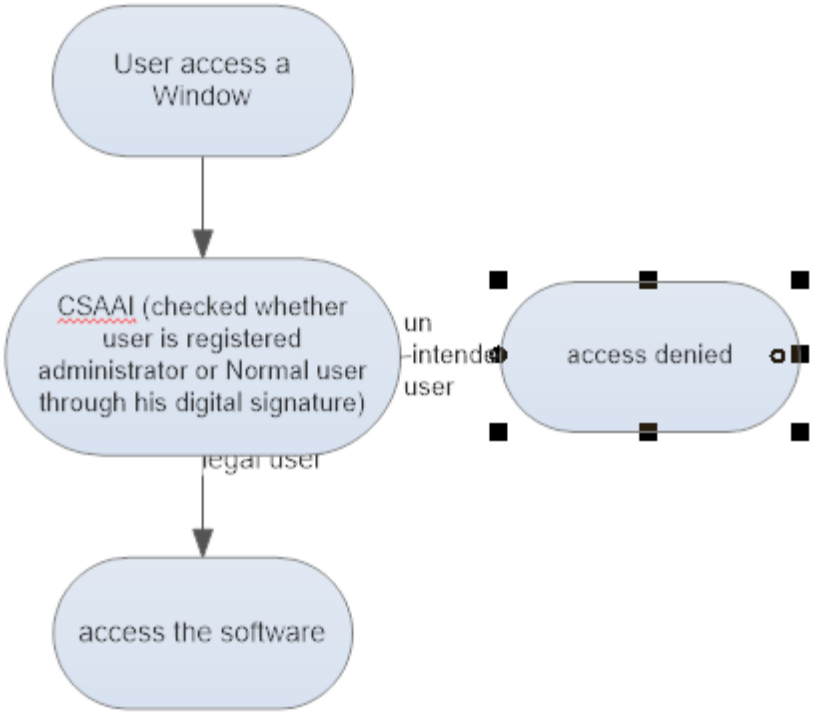

Fig 1: User Access Window

2) Encrypt and Decrypt of data

In this Integrated action is performed by scrambling the data using distinctive encryption techniques and interpreting systems, for instance, AES, DES, Two-fish, Blowfish, Serpent, IDEA, etc for giving Information Security., using DES encryption computation to encode and unscramble the substance of the record action. In Encryption, the key is embedded around the beginning of the data string, and are called initial round, this iteration did 9 normal rounds and ends with a final round which is slightly modified. At the time of normal rounds, a few operations are being performed like: Sub Bytes, Shift Rows, Mix Columns, and Add Round key. The last round is a normal round without the mix of columns stage. AES encryption is used in an application which needs sensitive data is being transmitted or transferred.

Communication Security

a) RFID Smart Card

c) ATM networks.

d) Encryption of Images

Storage Security

e) Highly Sensitive Data.

f) PSU Documents

g) Files related to crimes

h) Individual Stored Data

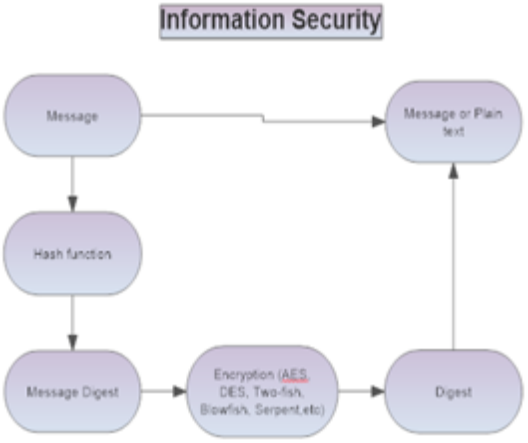

Fig 2. Information Security

Securing Network

It is absolutely perfect with IPV6 which bolster IP SEC layer for system and IP tends to security. In this, if there is any programmer included by means of recognizing obscure association with information put away at cloud then the earlier date will be given to the Client [7]. Structure security recollects the support of access to information for a system, which is constrained by the system head. Clients pick or are given an ID and secret key or other checking data that licenses them access to data and adventures inside their ability. System security covers a mix of PC structures, both open and private, that are utilized in ordinary occupations; driving exchanges and correspondences among affiliations, government work environments, and people [11] Networks can be private, for example, inside an affiliation, and others which may be available to the system. Structure security is identified with affiliations, undertakings, and different kinds of foundations. It does as its title clarifies: It guarantees about the structure, comparably as ensuring about and coordinating tasks being finished. The most for the most part saw and clear procedure for ensuring system assets is by conveying it an unprecedented name and a seeing secret key. [12].

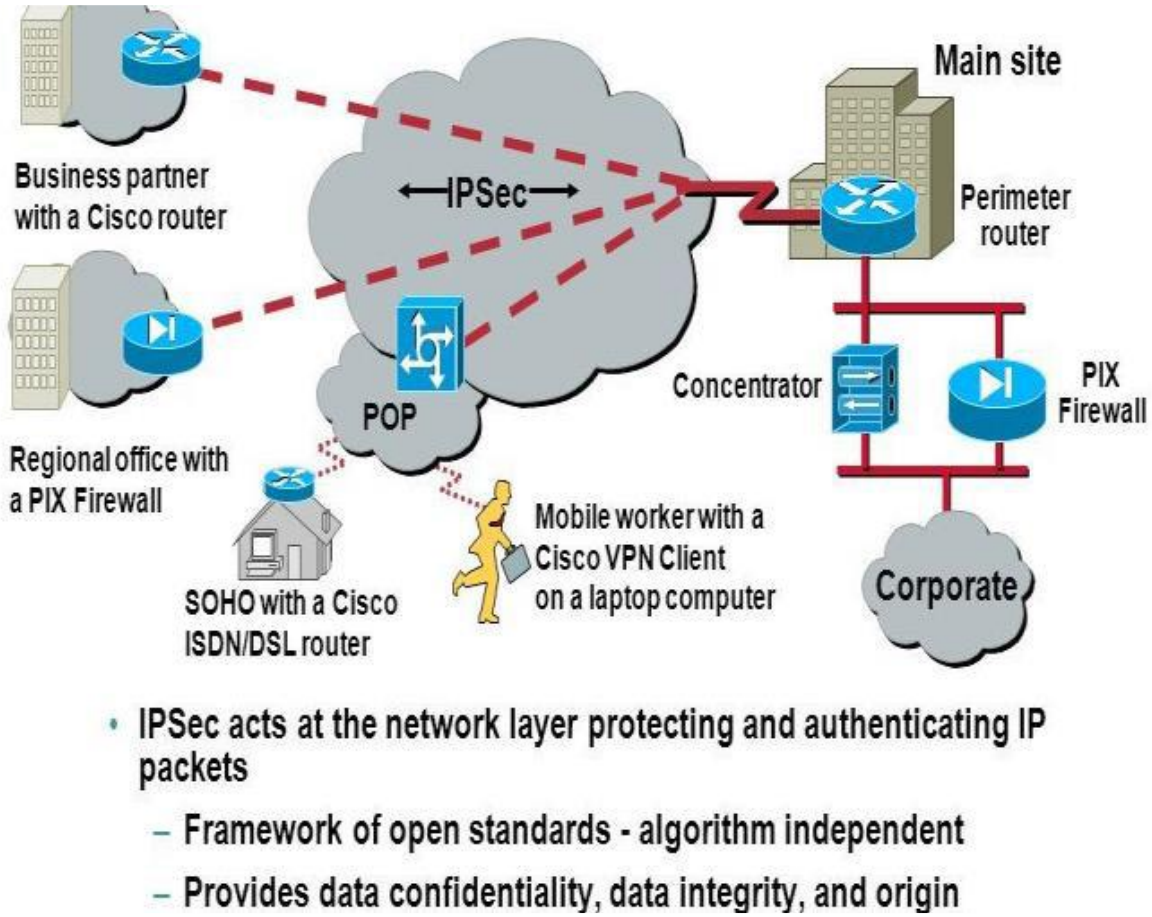

Fig 3: Framework for Security

III. FINAL RESULT AND CONCLUSION

In this paper we dissect that the procedure of encryption and unscrambling is perform by utilizing DES, AES and RSA calculations. In future we will apply and actualize these procedures for secure and better correspondence. On account of conventional strategies, we are just 60-70% sure of having digital security yet by means of utilizing this CSAAI we guarantee 90-100% digital security.