Study of Cyber Security and Artificial Intelligence

Pratibha (Btech Student) [1], Khushboo Khanna (Assistant Professor) [2]
[1]*CGC Technical Campus, Jhanjeri, Mohali Punjab*

***Abstract*—** In order to upgrade cyber security and provide unassailable cyber protection and attacks prevention, need of hour to introduce stringent "CSAAI". Artificial intelligence [9] is intelligence exhibited by machines, rather than humans or other animals (natural intelligence, NI). In computer science, the field of AI research defines itself as the study of "intelligent agents": any device that perceives its environment and takes actions that maximize its chance of success at some goal.[1] Colloquially, the term "artificial intelligence" is applied when a machine mimics "cognitive" functions that humans associate with other human minds, such as "learning" and "problem solving".

Keywords*—Coder Decoder, Airport security, explosive detection, Barcodes.*

1. INTRODUCTION

Cyber security is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In a computing context, security includes both cyber security and physical security. In 2017, the threat level to enterprise IT continues to be at very high levels, with daily accounts in the media of large breaches and attacks[3] such as credential reuse, Session Hijacking and Man in Middle Attack, Denial of Service, cross site scripting, SQL injection, Phishing, Malware, Password Cracking, IP spoofing, DNS spoofing, SMURF attack, SPAM emails, Masquerade attack, Replay attack, Traffic Analysis. So, in order to prevent from such kind of cyber attacks we require strong cyber security. Elements of cyber security[4] include Application security, Information security, Network security, Disaster recovery / business continuity planning, End-user education. Nowadays Information Security is provided with the help of encryption and decryption techniques such as AES,DES,2 DES, Triple DES ,Serpent, Two-fish, Blowfish, IDE and Authentication techniques such as Digital signatures,MD5,SHA1,etc algorithms. The Network Security is provided via using IPV6 internet protocol-security (IPSEC) layer. Large-scale cyber attacks continue to plague users, companies, and even countries. The WannaCry ransom ware attack encrypted users' data and demanded ransom payments in exchange for returning access to the data [1].Dyn, a company that runs the Internet domain name system for many leading sites, was the victim of a distributed denial-of-service (DDoS) attack, resulting in large parts of the Internet becoming inaccessible. And, the recent Petya cyber sabotage attack appears to be directed at systems in Ukraine but has spread to other countries. Software often meets functional requirements for consumer use but fails to build in security protections, leading to compromises and far-reaching unintended consequences. Built In versus Bolted on Much has been written about the impact of insecure software for everyday consumers. For example, insufficient security protections have led to the "evil grade" class of attacks against insecure software patching mechanisms, enabling the infection and weaponization of hundreds of thousands of everyday devices. These devices, such as webcams and DVRs, can then be deployed in attacks like the DDoS against Dyn. Although there are many facets of these incidents, attacks like these highlight the need to shift to secure system and software design and implementation that build in appropriate security protections from the beginning. The traditional software development lifecycle (SDLC) has often addressed security concerns in the testing phase, which results in very expensive fixes6 or, worse, security issues that aren't uncovered until operation. Secure development practices integrate security-related activities in each phase of the SDLC, yielding benefits by making security a continuous concern rather than simply part of test procedures. Many organizations 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 many advances have been made in secure coding practices such as penetration testing, secure code tools and analyzers, and exploit mitigation techniques [2].Yet these security advances run the risk of being underutilized. For security advances to be "built in" from the beginning, rather than "bolted on" at the end, security researchers must work with industry practitioners to learn the challenges of security in the engineering trenches and to build partnerships that mature and transition innovations from research to practice. Despite secure SDLC models and advances in secure development techniques, there are many open areas of research. Further, there's a gap between secure development research and secure development practices that must be addressed with both community building and new innovations.

A. Types of Cyber Attacks[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. Need of Artificial Intelligence in field of 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.

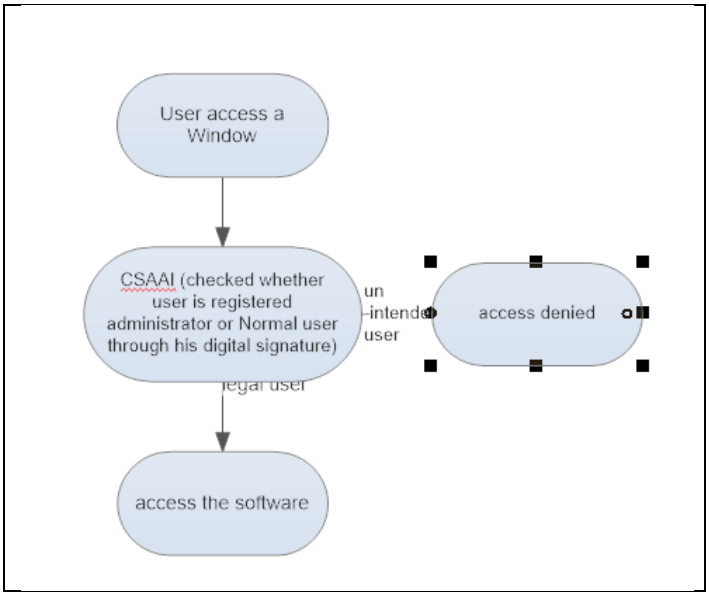
II. THE PROPOSED WORK

Big Data, Cloud Computing, IOT and Artificial Intelligence can be used to fight with cyber attacks. For this need of hour is to use "CSAAI " .

These are the Steps to be taken:

1) Log in:

After getting log in user will access a window and machine provided by artificial intelligence will take decision whether user who has logged into the website is legal or un-intended user and to block its access automatically without any human command and interference.If user is unintended then access to that user will be denied and if that person is normal user than that user is protected.



2) Encryption and Decryption

In this Integrated job is performed by encrypting the data using various encryption techniques and decryption techniques such as AES, DES, Two-fish, Blowfish, Serpent, IDEA etc for providing Information Security. , using DES encryption algorithm to encrypt and decrypt the contents of the file operation. In encryption mode, the initial key is added to the input value at the very beginning, which is called an initial round. This is followed by 9 iterations of a normal round and ends with a slightly modified final round. During one normal round the following operations are performed in the following order: Sub Bytes, Shift Rows, Mix Columns, and Add Round key. The final round is a normal round without the Mix Columns stage [10]

AES APPLICATIONS

AES Encryption and Decryption has many applications. It is used in cases where data is too sensitive that only the authorized people are supposed to know and not to the rest.

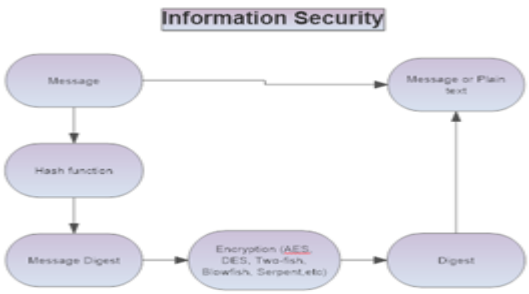
Secure Communication

a) *Smart Cards*
b) *RFID.*
c) *ATM networks.*
d) *Image encryption*

Secure Storage

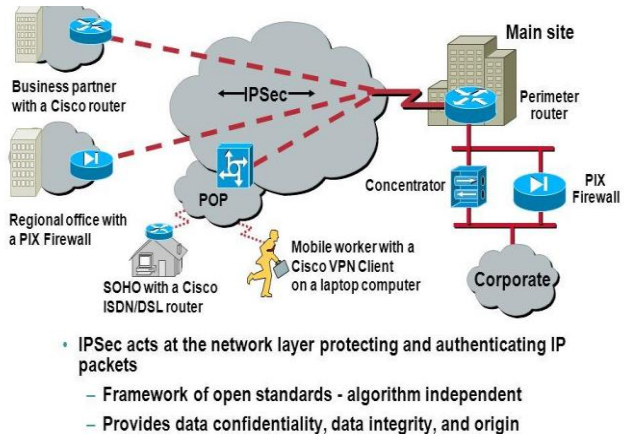
e) *Confidential Cooperate Documents*
f) *Government Documents*
g) *FBI Files*
h) *Personal Storage Devices*
i) *Person Information Protection*

-



Network Security

It is totally compatible with IPV6 which support IP SEC layer for network and IP addresses security. In this if there is any hacker involved via identifying unknown connection to data stored at cloud then the prior information will be given to the Client [7]. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals[11] Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password [12].



III. RESULT AND CONCLUSIONS

In this paper we analyze that the process of encryption and decryption is perform by using DES, AES and RSA algorithms. In future we will apply and implement these processes for secure and better communication. In the case of traditional techniques we are only 60-70% sure of having cyber security but via using this CSAAI we assure 90-100% cyber security.

IV. REFERENCES

[1] S. Hilton, "Dyn Analysis Summary of Friday October 21 Attack," Oracle+ Dyn, 26 Oct. 2016; dyn.com /blog/dyn-analysis-summary-of -friday-october-21-attack.
[2] https://www.google.co.in/search?q=definition+of+cyber+security&oq=definition+of+cyber+security&aqs=chrome..69i57j0l5.8515j0j4&sourceid=chrome&espv=2&es_sm=93&ie=UTF-8
[3] Gartnhttps://www.linkedin.com/pulse/pros-cons-artificial-intelligence-mike-fekety
[4] https://www.rapid7.com/fundamentals/types-of-attacks/
[5] http://whatis.techtarget.com/definition/cybersecurity
[6] https://www.youtube.com/watch?v=5ntcpEnyapI
[7] https://en.wikipedia.org/wiki/List_of_cyberattacks
[8] https://en.wikipedia.org/wiki/Artificial_intelligence.
[9] https://en.wikipedia.org/wiki/Network_security.
[10] Analysis and Review of Encryption and Decryption for Secure Communication.
[11] International Journal of Scientific Engineering and Research (IJSER) ISSN (Online): 2347-3878 Volume 2 Issue 2, February 2014.
[12] Implementation of Advanced Encryption Standard Algorithm International Journal of Scientific & Engineering Research Volume 3, Issue 3, March -2012 1 ISSN 2229-5518.