# Emotion Based Network Security Using Artificial Intelligence

[1]*Radhika Rajoju,* [2]*Dr. D. Sunitha*
[1]Assistant Professor, Department of Computer Science and Engineering, KITS, Singapur, Karimnagar
Telangana, India, Email: radhika.manu223@gmail.com
[2]Associate Professor, Department of Computer Science and Engineering, KITS, Singapur, Karimnagar
Telangana, India, Email: doddasunitha2004@gmail.com

## Abstract

The wireless networks are widely used in real-world applications. Innovations in wireless technologies are made wireless devices to become more possessive of resources. The result is in the form of wireless networks that can participate in many applications. But network security is an open challenge in wireless networks. The effect of cyber attacks is more in financial applications. Many researchers are introduced to different threat identification approaches in wireless networks. However, these approaches are unable to defend the current threat attacks. In this research work proposed a novel emotion-based network security mechanism using artificial intelligence. This security mechanism is technically connected user emotionally. The authentication is performed based on user emotional, and it's calculated by artificial intelligence. The results of experiments reveal the utility of the proposed emotion-based security mechanism

## 1. Introduction

Provide security is the main concern in wireless networks irrespective of the application and area of networks. There no use of network devices and applications without security. Security is an integral part of network devices and applications which are being developed. The cyber attacks are very complicated in wireless networks. Many network areas and individuals are victims of these cyber-attacks. The hackers are changing the behavior of attacks in wireless networks. The modern attack mitigation techniques are collaborating with the attacks and their behaviors at a single stage. At this stage, the attacks are clustered and analyzed by the machine learning algorithm of artificial intelligence[1].

The artificial intelligence plays a vital role in providing security in wireless networks. The artificial intelligence used in different applications such as attack detection, preventive attack and enhance reliability in the network computing[2].

The recent researchers are showing from database that most of the users are choosing low quality passwords. The sony database has given a report that by analyzing million passwords 50% of the passwords of different users are less than 8 characters out of these only 1% of passwords includes alpha numeric characters [9]. Although new password authentication process has improved the security and also improved the quality of network passwords too. Users are always finding the better and easy path in choosing the passwords like selecting the system given passwords, but these are outweigh the extra rework to select the strong password.

A massive-scale study of password use and re-use behavior got here to the belief that imparting instructions on a way to create cozy passwords, password managers, or offering tools inclusive of power-meters to enforce the electricity of a password had only limited achievement [10]. Many investigations tried to mitigate this to build a utility that will increase the security of a designated password by placing random characters. A browser extension that mingles the internet site to the password of the person, permitting him to reuse the same password for one-of-a-kind web sites. One of the maximum referred to papers on passwords is [11]. He defined key issues regarding password security (discern 2): length, composition, lifetime, and choice approach. One reveals that growing the length enhances the energy of a password exponentially, whereas growing composition complements it simplest linearly: cl where c denotes complexity, that means the opportunity for every role, and l denotes the period of the password.

## 2. Related Work

Enn Tygu et al[4], introduced constraint techniques to defense the cyber attacks in wireless networks. The technique is implemented using the neural networks, but the neural networks are not efficient in defense of cyber attacks.

Harini et al[5], proposed an intelligent system to prevent DDOS attacks in wireless networks. The intelligent system is worked with a combination of neural nets and expert systems. The system is worked efficiently in finding the malicious code of malware installation.

Mohana K.V[6], introduced a cryptographic technique to defend the cyber attacks. To provide the security it uses a genetic algorithm and chaotic neural networks. The genetic algorithm generates cryptographic keys and chaotic neural networks used to process the keys. The generated keys are used in data encryption and decryption.

L.N Wijesinghe et al. [7], proposed Intrusion Detection System (IDS). IDS used disruption and intelligence agents. The combined IDS detect cybercrimes. The system also preventive the attacks and raise the malware notification.

Anna L. Buczak [8] et al, proposed cyber analytics techniques to provide security in wireless networks. The cybersecurity algorithm is a combination of data mining and machine learning algorithms. However, these techniques are performed efficiently in the detection of cyberattacks. But the implementation of data mining and machine learning algorithms is complicated and cost-effective.

## 3. Proposed Methodology

### 3.1 Problem Statement

Many network security applications have different security mechanisms. The previous security mechanism is to identify or preventive the attacks in the middle of the application. The security applications are failures in the authorization. The previous researchers mainly used cryptography mechanisms and a two-level password mechanism. The first one is the cryptography mechanism used an algorithm to generate a secret key. This mechanism is mainly focused on matching keys only. The two-level password mechanism is focused on password matching only. The main problem in the previous mechanism is that it only followed authentication and authorization.

### 3.2 Emotion Based Security

The existing system implemented authentication and authorization using different algorithms. The algorithms are considered matching the input keys or password, but not user emotions. The hackers have utilized this defect and improve the cyber attacks in the network. In the proposed system, implement an emotion-based network security mechanism using artificial intelligence.

Applying high-quality feelings including joy and interest is possible through adding emoticons and wonderful messages; we use this approach to enhance password deciding on.

Usage of wonderful emotions using effective emotions enhances sociability, well-being, and positive conduct. Fantastic feelings prompt concept-motion repertoires, mitigate or undo the emotional effects of poor activities, and boom intellectual flexibility. Via the induction of fantastic emotions, it's miles viable to make use of them for preventive interventions.

Utilization of negative feelings poor emotions affect getting to know and reminiscence, “The amygdala’s affect on reminiscence ensures that emotional activities are also much more likely to be remembered through the years”. The amygdala is part of the brain answerable for dealing with emotions including fear, tension, and depression. It is also very crucial for memorizing connection among feelings and attention. A strong emotion turns on focus, focus turns on the operating memory and the working memory actives long-time period reminiscence, which is needed to consider passwords

We practice principles of aim framing and self-view to analyze how attitudes and norms may be manipulated. The overarching theories are nice and poor feelings. Inside the context of this take a look at, the framing of a message serves to recognition the individual either on preventing the hazard and related poor consequences of a protection violation (negative) or on the utilization of effective coping responses to create a safe, reliable internet environment (nice).

The mechanism maintains the information of each user with respective passwords.

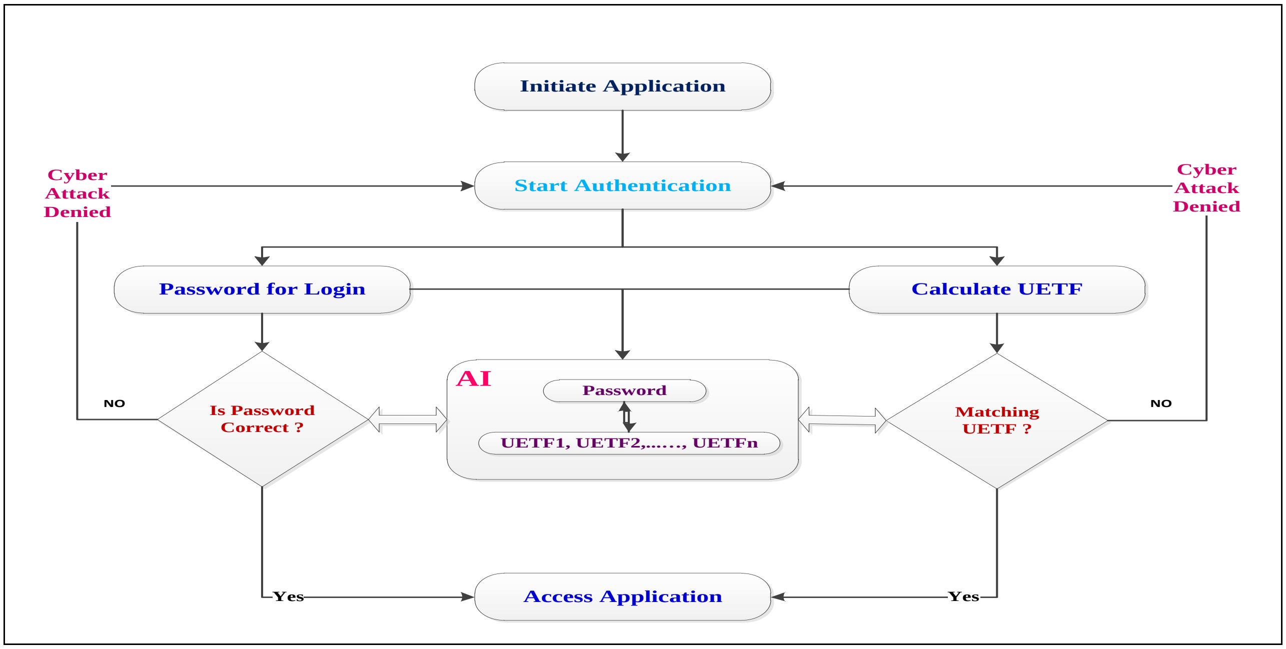


Figure 1. Architecture of Emotion Based Network Security Model

The emotion based security mechanism efficiently implements the authentication using artificial intelligence. The proposed emotion-based network security mechanism architecture can be observed in figure 1.

### 3.3 Algorithm

**Algorithm Name : Emotion Based Network Security Algorithm**

**Input :** Input Password *IPW*, Create Password *CPW*, Input *UETF*

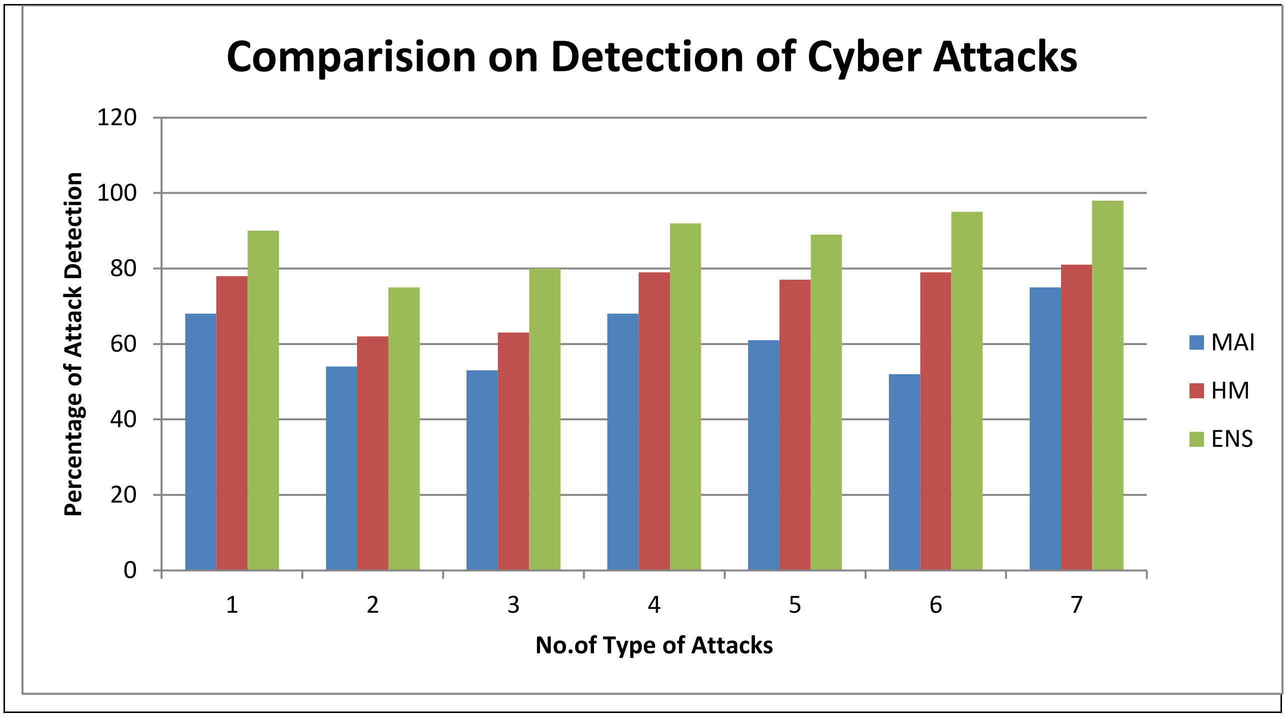
**Output :** Defend Cyber Attacks

```
Start
Initiate Application
Enter Password
Calculate UETF
Apply AI()
{
(CPW,(UETF1, UETF2,……,UETFn))
}
If(IPW == CPW) {
    If(IUETF == (UETF1,UETF2,……,UETFn)){
        Access Application
    } else {
        Defend Cyber Attacks
    } End If
else {
    Defend Cyber Attacks
} End If
End
```

The mechanism calculate each user's emotion in password typing. Using artificial intelligence maintain the user emotion in key typing with respective user password. The network security mechanism authenticates not only user password but also calculates user emotion. The artificial intelligence is efficiently working to maintain each user's emotion in password typing and password matching. The classifier easily identifies and prevents cyber attacks in network computing.

## 4. Result Analysis

In this, the section discusses the experimental results of the proposed mechanism. The different types of attacks denied by the proposed security mechanism in wireless networks. The proposed mechanism of cyber attack detection is compared with the previous system. The proposed mechanism achieved better performance. The benchmark performance of the proposed mechanism can be observed in figure 2.



In figure taken the Y-Axis as percentage of attack detection . The X-axis consider the different type of attacks such as 1. Network Scan, 2. Port Scan, 3. Enumeration, 4. Smurf Attack, 5. SYN Flooding, 6. Ping Flooding, 7. Session Hijacking. The proposed mechanism achieved high detection rate noticed in figure 2. as Enhanced Based Network Security (ENS), Multi Agent Intrusion Detection System(MAI) and Hybrid Method(HM)[3].

## 5. Conclusion

Artificial Intelligence is very essential for network security. The methods of artificial intelligence valuable for security applications. Many algorithms in artificial intelligence have mitigated the threats in reactive mode and do not consider the threat characteristics. In the proposed system, introduced a novel emotion-based network security mechanism. It calculates the emotion of each user in typing the password for authentication. The classifier allows only the user to match the password typing as well as password. The proposed mechanism defends the cyber-attacks proactively.

## 6. References

1. Li Wencui et al,. (2018). An Information Security Prevention System of Power Grid Enterprises Based on Artificial Intelligence. IEEE International Conference of Safety Produce Informatization (IICSPI). 1 (1), p148-152.
2. Boyang Zhang et al,. (2017). DDoS Detection and Prevention Based on Artificial Intelligence Techniques. IEEE International Conference on Computer and Communications. 1 (1), p1276-1280.
3. Georgi Tsochev et al. (2019). Improving the Efficiency of IDPS by using Hybrid Methods from Artificial Intelligence. IEEE. 1 (1), p1-4.
4. Enn Ty ugu et al ,. (2018) Artificial Intelligence in Cy ber Defense. Cyber Conflict.1(1), p1-6.
5. Harini M Rajan et al,. (2017) Artificial Intelligence in Cyber Security-An Investigation. IRJCS.9(4), p28–30, 2017.
6. Mohana et al. (2014) Data Security using Genetic Algorithm and Artificial Neural Network. IJSER 5(2). p543–548.
7. L.S.Wijesinghe et al,. (2014 ) Combating Cy ber Crime Using Artificial Agent Systems. IJSR Publication 6(4), p265-271.
8. Anna L et al,. (2016) A Survey of Data M ining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE Communication, vol. 18, no. 2, p1153–1176.
9. Hunt, T, “A brief Sony password analysis”, available at: www.troyhunt.com/2011/06/brief-sony-password-analysis.html, 2011.
10. Florencio, D. and Herley, C, “A large-scale study of web password habits”, Proceedings of the 16th international conference on World Wide Web, ACM, New York, NY, 2007.
11. Zviran, M. and Haga, W.J. (1999), “Password security: an empirical study”, Journal of Management Information System, Vol. 15 No. 4, pp. 161-185.