Wifi Audit for Wireless Network using AI Generated Passwords

[1]Nida Noorain, [2]Dr. Nirmala S

[1]MTech Scholar, [2]Professor

[1, 2]CSE Dept.

[1,2]AMC Engineering College, Bangalore, India

Abstract: HashCat and John the Ripper are most generally used password cracking tools employed by users to crack large set of passwords in shorter time span. Although these techniques can be used but to create, expand and to consider various datasets requires special training and experience, moreover they are time consuming and labor-intensive process. To address this issue, we use PassGAN to audit wireless networks. They are designed to use the machine learning algorithms to learn the characteristics and distribution pattern within a dataset and to derive a similar looking dataset instead of making use generated password rules. PassGAN employ a Generative Adversarial Network (GAN) which consists of a generator and discriminator instead of depending on manual analysis to automatically learn from the training dataset and to produce a similar password guesses list which closely matches the user to audit the network and for cracking the passwords of wireless networks.

Keywords: PassGAN, Handshakes, Generator, Discriminator, Aircrack-ng.

1. INTRODUCTION

In the recent era, wireless technologies have come into picture and because they provide many opportunities and use cases, large number of devices are being connected to wireless networks or Wi-Fi organizations. Out of all the use cases it is highly important to provide security to the devices and the wireless network. Wireless networks utilize radio waves to ship information from one place to another and using these radio waves it is easier for the attackers or hackers to perform attacks on devices, they will be able to learn delicate data, send malignant information to network devices and can even sidestep firewalls. For this reason, we make use of security inspecting and penetration testing in order to increase the protection for wireless networks and devices from the attackers. Wi-Fi Auditor is an assortment of Wi-Fi testing devices and software services which are bundled jointly inside Raspberry Pi 3 module. This tool permits the ethical hacker and penetration tester for surveillance on the particularly chosen customer, or it can be done in a combined manner.

The password has become the present prevailing technique for verification. Although numerous validation strategies, password protection is viewed as the most dominant technique. Passwords are significant for both assailants and for legal ethical hackers relying upon their viewpoints. There are a few plans created against offline assaults, so the breaking of secret phrase gets more earnestly. In our project make use of PassGan, a new philosophy that makes use of machine learning algorithms instead of depending on man-made rules for secret key or depending on any kind of intuition. PassGan makes use of a generator network and a discriminator network which are a Generative Adversarial Network (GAN) to get comfortable with assignment of authentic secrets keys with a collection of real mystery key breaks automatically, and to create top type secret word deduces.

2. LITERATURE SURVEY

In paper [1], Edward C. Lo and Mike Marchand, to introduce the basics of data frameworks security review through a genuine security review done on a medium-sized association. The audit was the principal security review done on the organization and would fill in as a security standard for future reviews. A successful security review ought not be a one-time shot yet rather a progressing cycle. Top, security is a fragile equilibrium among protection, accessibility and client acknowledgment. They start the security review at the outside of the organization and slowly work our direction internal. A vulnerability check is played out on the uncovered IP locations and ports. Every one of the vulnerabilities found was painstakingly surveyed to check whether it disregarded the security approaches of the association. This paper helps us to understand the importance of security audit to be done on an organization and the direction on which it must be conducted.

In paper [2], Priyash Shinde, bhijeet Karve , Paras Mandaliya , Prof. Sandesh Patil, In the recent era, wireless technologies have come into picture and because they provide many opportunities and use cases. The one of the most general worries regarding wireless networks are protection of the network and the data, which is of utmost importance to the end users. Wi-Fi Reviewer consists of assortment of testing apparatuses and administrations. Reviewer permits entrance analyser along the line of directing assaults to observe a particular chosen customer otherwise an organization. Reviewer is convenient, covertness, fast henceforth permitting the assailant to re-enact the assaults without anybody seeing them. Wi-Fi examiner helps the developers and programmers in an organisation by warning them of the possible attacks that can take place by the assailants and to reduce the dangers from hackers. It is also helpful to log this information so that it can be available in future and provides guidance for the future designers.

In paper [3], Jai Narayan Goel, BM Mehtre, Intricacy of frameworks are being grown and this triggers to identify the weaknesses in Systems. Aggressors learn from these weaknesses so that they will be able to launch an attack to a system or an entire organisation to misuse the casualty's framework. Therefore, its considered smarter to find these defects in the system and a network before an attacker tries to hack the system and to improve the authentication methods and security so that it is strong enough to stop the attacks. The force of Vulnerability appraisal is typically disparaged. While Vulnerability Assessment and Penetration Testing can be utilized as a digital safeguard innovation to give proactive digital protection. In this paper Vulnerability Assessment and Penetration Testing (VAPT) as a Cyber guard innovation is studied, how we can give dynamic digital protection utilizing Vulnerability Assessment and Infiltration Testing.

3. EXISTING SYSTEM

Passwords form an important part of authentication in wireless network security and therefore passwords must be protected from attackers. Passwords that can be hashed is a form of typical speculating strategy. While brute-force assault strategies, for example, JtR and HashCat demonstrated strange behaviour and unpractical to use, the exploration at that point changes to password speculating strategies. In 2009, Probabilistic context free grammar (PCFG) was used by Weir et al to perform the cracking of passwords. These grammar-based methodology make use of rules to parse the structures to match the target password.

Disadvantages

- Probabilistic context free grammars (PCFG) and Markov models were used extensively, but these methods require a lot of computation which is tedious.
- For Hashing Passwords, John the Ripper and HashCat are generally but are found to be unpractical and requires specialised expertise.
- Existing systems are specially appointed and dependent on instincts on how clients pick secret phrase, but the earlier methods do not perform principled investigation consisting enormous secret phrase.

4. PROPOSED SYSTEM

- Wireless network passwords can be cracked from pre-captured handshakes.
- The network card must be placed in monitor mode to capture packets in the network.
- Wireless network passwords can be extracted from these handshakes by using Aircrack-ng.
- Deep learning techniques are used to generate a wordlist containing passwords which is used to crack the passphrase efficiently.
- Password suggestions to help strengthen the network.

Advantages

- Project makes use of PassGan which uses machine learning techniques and rules instead of the basic human generated passwords.
- Rather than depending on manual secret key investigation, PassGAN utilizes a Generative Adversarial Network (GAN) to self-governing gain proficiency.
- Our method does not require any prior knowledge of the password structures to crack the password.
- PassGan is found to extract additional properties from the passwords when compared to the existing password guessing strategies.

5. SYSTEM DESIGN

The design of the system comprises of six stages as shown in fig.1, in the first stage the model makes use of the leaked password dataset. The dataset used in this project is the RockYou dataset. This dataset is used to train the model of the neural networks. This is given to the PassGan Architecture which has a generator and the discriminator, they make use of Generative Adversarial Networks which automatically learn the passwords from the leaked passwords dataset provided as input and they generate similar high-quality passwords which constitute the probable wordlist which is used for cracking the password.

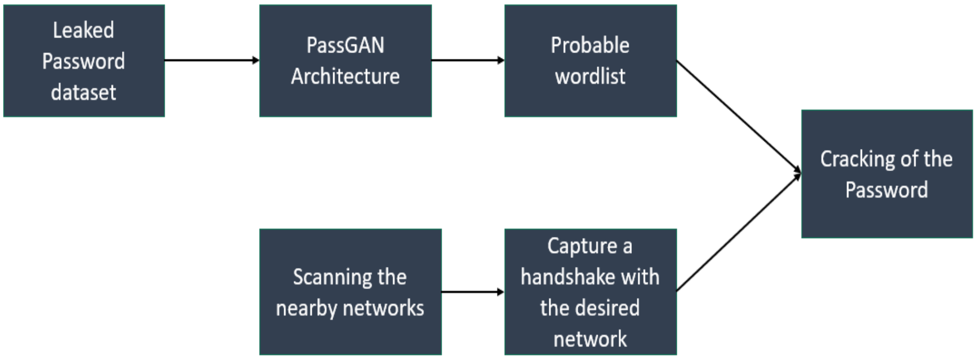


Figure 1: System Architecture Diagram

The nearby networks are scanned in the area and displayed to the user, the user selects the desired network he wishes to perform the audit and starts the audit by capturing the handshake. Once the handshake is captured or if there are any pre-stored handshakes the auditing begins by scanning all the passwords in the probable wordlist and if the password is present in the wordlist, then the password is cracked.

5.1ROCKYOU DATASET

The RockYou dataset is used for training the model which approximately has 32,503,388 passwords. In order to train the model, we will use all passwords in the list which has a size of 10 or less characters. Which relate to around 90 percent of the dataset.

5.2 PASSGAN ARCHITECTURE

PassGAN, is a new and fresh methodology that makes use of hypothesis grounded AI calculations rather than depending on the manmade rules or instincts to generate the passwords. Rather than depending on manual secret key examination, PassGAN utilizes a Generative Adversarial Organization (GAN) to self-sufficiently get familiar with the conveyance of genuine passwords from genuine password spills, and to produce top caliber secret key guesses. PassGAN accomplished this outcome with no deduced information on passwords or basic secret phrase structures. GANs are as of late acquainted AI devices planned with perform thickness assessment in high-dimensional spaces at its center, our thought is to prepare a neural organization to decide self-sufficiently secret word attributes. The architecture of PassGAN is represented in below fig.2.

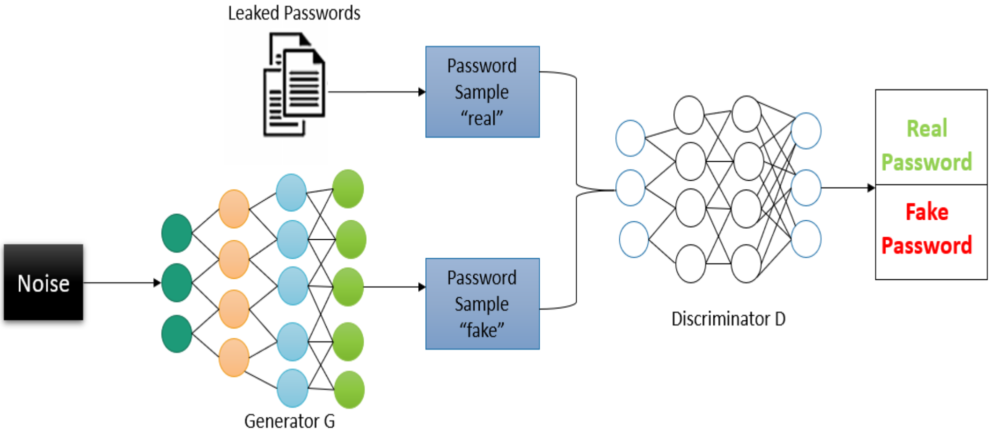


Figure 2: PassGAN Architecture Diagram

5.3 WPA HANDSHAKES

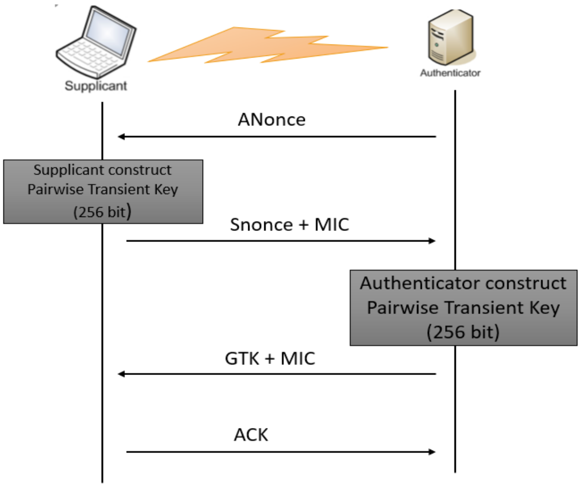

Supplicant
Authenticator
ANonce
Supplicant construct Pairwise Transient Key (256 bit)
Snonce + MIC
Authenticator construct Pairwise Transient Key (256 bit)
GTK + MIC
ACK

Figure 3: WPA Network Authentication

Wireless customers and the AP utilize a four-way handshake that utilizes the pre-shared key as contribution to create encryption 802.11i confirmation utilizing the entrance of EAP convention, that incorporates 3 affirmation substance validation worker (AS verification worker), authenticator (AP validation point) and site (ST A station) and the in the accreditation interaction Access Point assumes part of validation information parcel, as well explicit certificate finished connecting the Authentication server and the Station A, after validation is finished an expert key is produced This Pair wise Master Key is exchanged between the Authentication server and the client in 4-way handshake convention. A Pair Wise Transient key is generated between the two recipients using the various key generation schemes. The various parameters and the method of generation of Pairwise Transient Key is shown in fig.3. All the exchanges between the two parties takes place using Extensible Authentication Protocol over LAN.

5.4 CRACKING PASSWORDS

Aircrack-ng is a suite containing tools for cracking passwords. This is mainly used for monitoring of the data traffic, sending of packets, to launch the attacks like replay attack, packet interception, password cracking that basically deals with WPA networks or improved version.

The encryption keys which are generated and previously shared among the components are used by the client as well as the authenticator to start communicating with each other when first the customer or client connects with the source. At the start of the communication a 4-way handshake is performed between the two parties. Airodump-ng helps to capture this four-path handshake. The other prerequisite for this type of attack is to have a probable wordlist of the passwords. At the start of four-path handshake, a de-authentication messages are sent to all the clients, this is done to speed up the capture of the packets to deduce the password. On the off chance that it does, the pre-shared key has been effectively recognized.

6. SYSTEM IMPLEMENTATION

The project has been implemented in Windows operating system, Raspbian OS and Python language. In this project we are making use of raspberry pi which is connected as shown in fig.4 because it is small in size and portable which is an essential requirement in our project, so that we can go about finding the available networks without having to worry about carrying a huge size system. The network adapter is used to inject and capture the packets into the network in monitor mode so that we can send DE authentication messages to the network to capture the handshakes. Once the handshakes are captured, it is possible to start the attack to crack the password.

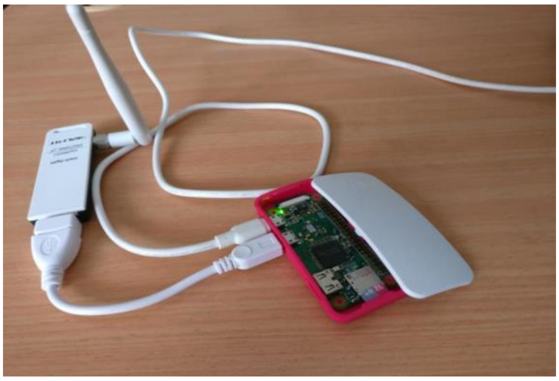


Figure 4: Raspberry pi connected with network adapter

7. FLOW CHART

The working flow of the system is shown in fig.5, The user logs into the system starts a 4-way handshake with the desired access point and if there is no handshake it starts capturing the desired handshake, if handshake is available, it will upload and runs aircrack-ng to guess the probable password it is then passed to generate a password through PassGan logic.

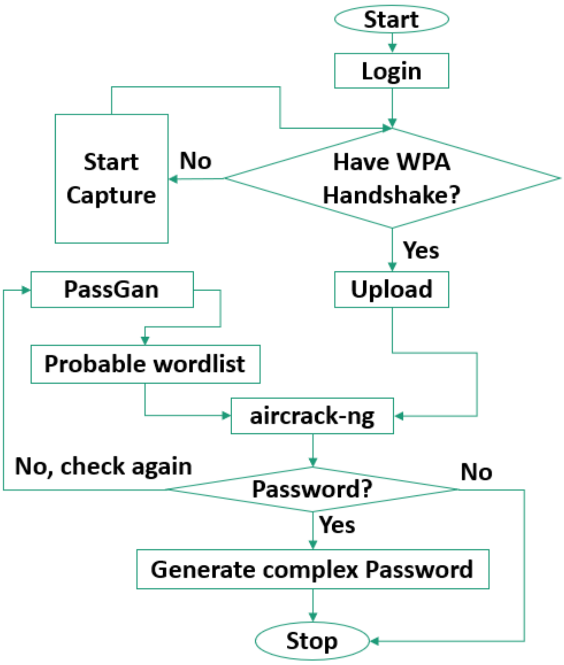
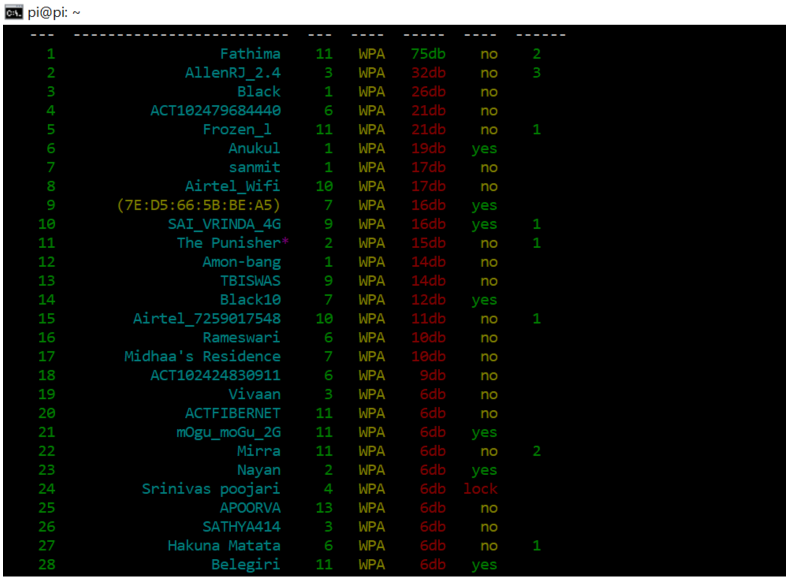


Figure 5: Flow chart diagram

8. RESULTS AND SNAPSHOTS

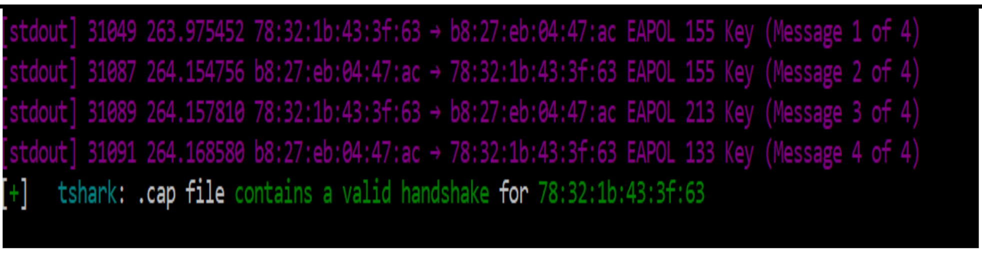
This chapter provides the results of the running project, where the user has to power on the raspberry Pi, connect the network adapter to the pi and put it in the monitor mode using various commands. Now we will be able to intercept or inject the packets travelling in the network.



```
 ---  ------------------------  ---  ----  -----  ----  ------
   1                   Fathima   11   WPA   75db    no     2
   2               AllenRJ_2.4    3   WPA   32db    no     3
   3                     Black    1   WPA   26db    no
   4           ACT102479684440    6   WPA   21db    no
   5                 Frozen_l    11   WPA   21db    no     1
   6                    Anukul    1   WPA   19db   yes
   7                    sanmit    1   WPA   17db    no
   8               Airtel_Wifi   10   WPA   17db    no
   9       (7E:D5:66:5B:BE:A5)    7   WPA   16db   yes
  10             SAI_VRINDA_4G    9   WPA   16db   yes     1
  11              The Punisher*   2   WPA   15db    no     1
  12                 Amon-bang    1   WPA   14db    no
  13                   TBISWAS    9   WPA   14db    no
  14                   Black10    7   WPA   12db   yes
  15         Airtel_7259017548   10   WPA   11db    no     1
  16                 Rameswari    6   WPA   10db    no
  17        Midhaa's Residence    7   WPA   10db    no
  18           ACT102424830911    6   WPA    9db    no
  19                    Vivaan    3   WPA    6db    no
  20               ACTFIBERNET   11   WPA    6db    no
  21              mOgu_moGu_2G   11   WPA    6db   yes
  22                     Mirra   11   WPA    6db    no     2
  23                     Nayan    2   WPA    6db   yes
  24          Srinivas poojari    4   WPA    6db  lock
  25                   APOORVA   13   WPA    6db    no
  26                 SATHYA414    3   WPA    6db    no
  27             Hakuna Matata    6   WPA    6db    no     1
  28                  Belegiri   11   WPA    6db   yes
```

Figure 6: Scanning of available nearby networks

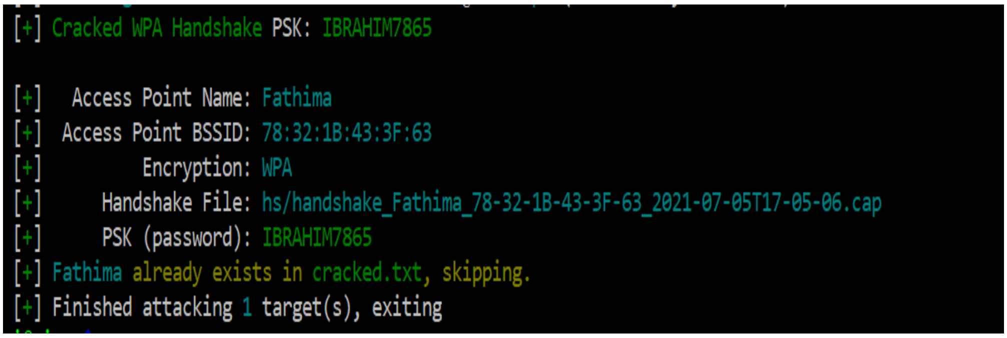
In the above fig.6, the nearby available networks are scanned and presented to the user. The user selects the desired network from the available networks and can start the handshakes for further password cracking.



```
[stdout] 31049 263.975452 78:32:1b:43:3f:63 → b8:27:eb:04:47:ac EAPOL 155 Key (Message 1 of 4)
[stdout] 31087 264.154756 b8:27:eb:04:47:ac → 78:32:1b:43:3f:63 EAPOL 155 Key (Message 2 of 4)
[stdout] 31089 264.157810 78:32:1b:43:3f:63 → b8:27:eb:04:47:ac EAPOL 213 Key (Message 3 of 4)
[stdout] 31091 264.168580 b8:27:eb:04:47:ac → 78:32:1b:43:3f:63 EAPOL 133 Key (Message 4 of 4)
[+]  tshark: .cap file contains a valid handshake for 78:32:1b:43:3f:63
```

Figure 7: Captured four messages of 4-way handshake

The above fig.7 shows the four messages captured during a four-way handshake that contains the encryption keys used the encrypt the data packets travelling within the network. The fig.8 shows the password cracked along with the details pertaining to the network.



```
[+] Cracked WPA Handshake PSK: IBRAHIM7865

[+]   Access Point Name: Fathima
[+]  Access Point BSSID: 78:32:1B:43:3F:63
[+]          Encryption: WPA
[+]      Handshake File: hs/handshake_Fathima_78-32-1B-43-3F-63_2021-07-05T17-05-06.cap
[+]      PSK (password): IBRAHIM7865
[+] Fathima already exists in cracked.txt, skipping.
[+] Finished attacking 1 target(s), exiting
```

Figure 8: The cracked Password details

9. CONCLUSION

In this undertaking, PassGAN is utilized to Wi-Fi Audit Wireless Organizations, PassGAN is the principal secret key speculating strategy dependent on generative Adversarial Networks (GANs). PassGAN will gain from a secret key dissemination data from a secret phrase list. Therefore, not at all like current secret word speculating instruments, PassGAN doesn't depend on any extra data, like unequivocal principles, or presumptions on the Markovian design of client picked passwords. I accept that our way to deal with secret word speculating in Wi-Fi Examining is progressive in light of the fact that PassGAN creates passwords with no client intercession, in this manner requiring no area information on passwords, nor manual examination of secret word records.

10. FUTURE SCOPE

In this project we make use of a model which learns from a dataset to generate similar passwords which resembles the actual dataset. In our future work, the main focus should be on training our model with multiple datasets so that the generated wordlist provides good results and accuracy with varied kinds of datasets trained not with single language dataset using similar kind of procedure for generating the password. It's accepted that password speculating requires further examination, as password validation won't be completely swapped for some time. Notwithstanding, the shortage of preparing assets remains an issue. In view of existing security conventions, it's important to restrict admittance for genuine passphrases, particularly required for preparing and testing. For this reason, we can tackle this issue, by adding extra databases in different dialects which constitute transfer learning.

ACKNOWLEDGMENTS

Our thanks to Mr. Maaz, Member of Technical Staff -III R&D, Mitel for his support in making this paper.

REFERENCES

[1] Edward C. Lo and Mike Marchand, “Security Audit: A Case Study”, IEEE, 2004.
[2] Priyash Shinde, Abhijeet Karve , Paras Mandaliya , Prof. Sandesh Patil, “Wireless Security Audit & Penetration Test using Raspberry Pi”, 2018.
[3] Jai Narayan Goel, BM Mehtre, “Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology”, 3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015).
[4] Shao-Long WANG, Jian WANG, Chao FENG and Zhi-Peng PAN, “Wireless Network Penetration Testing and Security Auditing”, 2016.
[5] Senbai Dalabaev , Sun quanfu , Li qinghua, He zhupingl ,Yue shilian, Abdiakhmetova Zukhra, “4-way handshake attack analysis and improvement in 802.11i”, CSQRWC, 2013.
[6] K. Kanchan Devi, S. Arumugam, “Password Cracking Algorithm using Probabilistic Conjunctive Grammar”, IEEE, 2019.
[7] Ragib Hasan, Shams Zawoad, Shahid Noor, Md Munirul Haque, and Darrell Burke, “How Secure is the Healthcare Network from Insider Attacks? An Audit Guideline for Vulnerability Analysis”, IEEE, 2016.
[8] Briland Hitaj, Paolo Gasti, Giuseppe Ateniese, Fernando Perez-Cruz,” PassGAN: A Deep Learning Approach for Password Guessing”, arXiv:1709.00440v3 [cs.CR], 14 Feb 2019.
[9] Vernit Garg, Laxmi Ahuja, “Password Guessing Using Deep Learning”, 2nd International Conference on Power Energy, Environment and Intelligent Control (PEEIC), 2019.
[10] Raspberry Pi, https://en.wikipedia.org/wiki/Raspberry_Pi