Risk Analysis of Putting Attacks into Perspective and Conducting a Vulnerability Assessment

Bhagya Rekha Kalukurthi
R & D Engineer3, Broadcom Inc,
India

***Abstract*- In various other to prevent unauthorized use risk set up via vulnerable wireless accessibility areas, Wired Matching Personal privacy - a low-level files shield of encryption physical body-- was developed for wireless security purposes. WEP protocol protects link-level information throughout wireless transmission in between consumers along with access to aspects. It carries out indeed certainly not give end-to-end security, nevertheless merely for the wireless area of the link. Wireless security is an authentic barrier for network managers and also particulars security managers similar. Unlike the wired Ethernet LANs, 802.11-based wireless LANs broadcast radio-frequency (RF) records for the customer terminals to pay attention to. As a result, anybody along with the right resources can quickly take hold of and also move wireless signs if he is in fact within a selection.**

***Keywords*- Vulner abilities, wlan, wireless networks.**

I.INTRODUCTION

WEP utilizes the circulation cypher RC4 for discretion, in addition to the CRC-32 checksum for integrity. The file shield of encryption secrets has to match on both the consumer and also acquire accessibility to direct for building exchanges to prosper. WEP might be conducted in 64 or 128 little bit of settings, whereby the WEP secrets utilized are generally40 and even104 little bits long, paired along with a24 little initialization vector(IV).WEP poss esses many known susceptibilities originating from its use of taken care of tricks, and a selection of weak initiali zation vectors.

A fan of WEP is Wi-Fi Protected Gain Access To (WPA). Delivered in 2003 as an advanced beginner step to change WEP while 802.11 I was readied, WPA steers clear of from a lot of WEP's susceptibilities using making a lot more significant use of dynamic/temporal secrets, taking advantage of the Temporal Top Secret Stability Operation (TKIP). It secures files taking advantage of the RC4 stream cypher, together with a 128-bit trick and also a 48-bit initialization angle (IV).

Validated on 24June2004,Wi-Fi Protected Gain Access To 2 (WPA2) is the follow-on security technique to WPA. WPA2 uses the Advanced File file encryption Require ment(AES).There is practically no identified wireless attack versus AES.CCMP is the security criterion made use of via AES. CCMP calculates a Notice Honesty Check (MIC) making use of an evaluated Cipher Block Chaining (CBC) tactic.Details are safeguarded making use of a 128-bit top-secret key and also a128 little bit block of information. The result is a risk-free security device.

This part analyzes the existing identified IEEE 802.11 wireless LAN susceptibilities as well as likewise dangers. It ends up together with sections that particular how to find wireless network dangers, as well as what to carry out to minimize or even remove the risks. Security bodies of wireless LANs are undoubtedly not within the level of the particular job. The reason is actually to motivate network and security administrators to conduct hazard assessment so involving recognize the threats and additionally threats connecting to their info device as well as after that set up adequate management measures to lower or even do away with a possible risk.

II. PUTTING ATTACKS INTO PERSPECTIVE: RISK ANALYSIS

The risk is probabilities of dangers in obtaining benefit from concerns or weakness which are a source of reductions and damages to properties or even teams of resources, effecting an institution directly or even in a round about way.Risk review is a growing source of WLAN hazard monitoring. Using this an outstanding security plan can be derived and likewise applied to justify the WLAN versus achievable attacks.

On-going monitoring, as well as frequent screening, may after that be used to verify that a launchedWLAN fulfils defined goals.Vulnerabilities revealed while doing this go to that aspect(re)researched,for that reason as to make clear the policies as well as provide remedies.This recurring procedure is high lighted in the design(fig1) sho wn listed below.

It is extremely vital to recognize the attacks that may affect a network. However, it has to be kept in mind that some incidents are much a lot less very likely or additional damaging than others. A lot more likewise, it requires to be even made note that it is not sensible or feasible to guard any kind of network versus all possible attacks. A more useful objective is actually to decrease the associated threat to a proper volume.Threats are taken into pers pective with calculating one's very own WLAN's suscepti bilities-the likelihood that a challenger is heading to manoeuvre them-along with business impact,will most certainly cultivate. The sticking to steps/points are called for in carrying out threat study

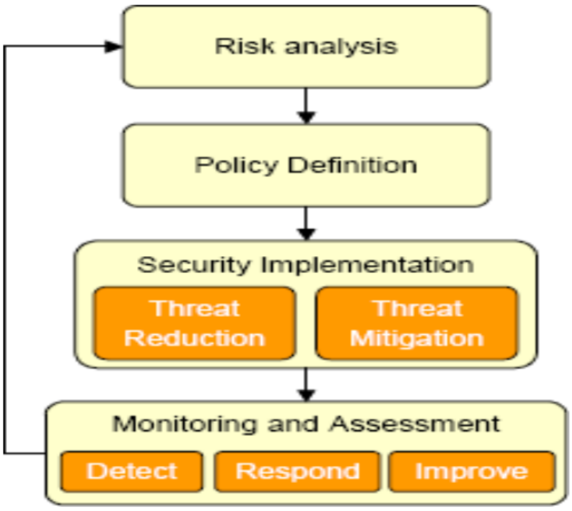


Fig 1. Security as a Process.

Define company demands
A record that needs to possess WLAN accessibility, as well as likewise where?
Recognize individuals or teams allowed to take advantage of 802.11 at the office while steering, along with in the residence.
Determine resources communicated to over wireless
Which applications, data sources, as well as parts must level to wireless consumers, along with when?
Next off, assess new company risks brought on by including wireless.
What details do those services and also information finan cial institutions feature?
Consider data that dwells on wireless terminals as well as additionally circulates over wireless internet links
For each information, predict the probability of concession as well as the additional potential cost to the company, using quantifiable metrics like recovery time, recovery expenses, etc.

Completion of this approach provides a prioritized list of at-risk information. Base upon this, a security planning that safeguards essential ownershipscoming from wireless borne attack,chiming with cost/benefit as well as also persisting hazard might be made.Upcoming action is actually to pick, position, as well as configure counter measures that apply and also apply the security plan.

III. CONDUCTING A VULNERABILITY ASSESSMENT

A sensitivity evaluation is a particular research study that uses seepage screening and likewise observing to identify security weaknesses that might be exploited,and additi onally the risks.The results acquired are actually after that assessed to learn strength as well as measures to reduced and even get rid of the risks. To become practical, exami nations must be performed regularly to find out newly introduced susceptibilities as well as validate that placed security techniques are working as organized. Examina tions may be performed through the interior or even third event crew, in addition to total, partial, or even no knowl edge of the affiliation network and additionally safe execution.

In the adhering to areas,I deliver the strategies and also devices that could be sensible for executing a WLAN weak spot evaluation:coming from wireless device looking for and likewise seepage screening process, to security event monitoring and also even realm evaluation. An example worksheet, supplied in the appendix, highlights only how analysis results can be recorded for customer testimonial as well as additionally removal.

IV. WLAN DISCOVERY

The 1st interfere with any kind of sort of sensitivity research is the identity of all wireless devices near the internet website(s) under examination.Through conseque ntly executing, all accredited firms are going to certainly be split up stemming from the rest- whereas the accredited will certainly go through added assessment; the remainder will undoubtedly be had a look at to develop possession, influence on WLAN operation, as well as also potential danger.

Wi-Fi Stumblers- which are free, easy for basic work, as well as also available for several Systems-- is amongst the devices that could be utilized for this feature.One restriction of Stumblers is definitely that they may swiftly locate APs, however certainly not Terminals or even non 802.11 challenge information. They might provide DIRECTION FINDER latitude/ longitude, nevertheless, might certainly not find in our property region.For total vulnerability examination,a mobile phoneWLAN Analyzer that might inspect all Superhigh frequency networks, export details regarding all wireless sources, suitably body leads on layout, as well as make it direct to find newly-discovered resources is excellent.

Benefiting from the advancement devices, assistance produce a checklist of monitored 802.11 in addition to countless other gadgets. Videotape the following specifications:a)forAPs,record their ESSID,MACINTOSH DESKTOP COMPUTER handle, Web Protocol takes care of, network, SNR, along with monitored 802.11/ 802.1 X setups, b)create a comparable list of identified Terminals, keeping in mind whether they are connected to an Unpla nned nodule, penetrating for several ESSIDs, as well as likewise about certain AP(s). For non-802.11 gadgets, a variation review is utilized to finger printing kind.To discover and likewise recognize the unjustified tools- including the owner-, utilize a "find" system(or WIPS along with artificial administering).

V. VULNERABILITY/PENETRATION TESTING

The essential aim at of seepage assessment remains in truth to establish places of the establishment network where trespassers can conveniently make the best use of security weak spot. These analyses are usually carried out utilizing automated devices that search for particular weaknesses, specialized concerns or maybe weak spot to use, with the results provided to the system operator with an analysis of their risk to the on-line setting and likewise a removal technique highlighting the tasks required to must eliminate the presences. Many sorts of infiltration assessment are crucial for different types of network units. As an example, an infiltration physical exam of firewall software plan is various coming from an infiltration observation of a traditional person's manufacturer. Even an intrusion examination of tools in the DMZ (demilitarized place)is several originating from executing an examination to discover whether network seepage is achievable. The sort of seepage exam has to be analyzed against the market place worth of the appropriate information on the creator being found out along with the criteria for the relationship to an offered company.

Tools like Nmap or perhaps Superscan are made use of to surf devices and also ports.Energetic gizmos are finger printed to identify running body system devices,web hosting server devices,accounts,as well as additionally slices taking advantage of information like Winfinger print and likewise Xprobe. WEP web traffic may be examined besides a source like Aircrack-btw, while PSK proof parti culars might be examined together with Chowpatty. 802.1 X/EAP buyer I.d.s could be recorded, along with additi onally password-based EAPs could be evaluated making use of a resource like Asleep.

1. Utilizing Wireless Invasion Security Physical Body to Keep an Eye on Task:

WIPS is a network keeping an eye on a source that oper ates night and day and also determines attacks or even found attacks on the wireless network.It is,in fact,a growth of the inventive security positioned in wired firewall system software program use as well as additionally virtu al personal network security physical bodies having said that, along with taking notice of wireless computer network(WLANs).It makes use of guest web website traffic assessment to track attack trade marks, approach miscalculations,erratic methods, and also program infrac tions,creating red flags as well as likewise protective tasks. Within a used RF band, WIPS noticing bodies listen thoroughly to the sky- both in the city as well as outlying workplaces- translating 802.11/ 802.1 X protocols and evaluating all wireless task. WIPS internet hosting servers recognize wireless attacks and also furthermore might execute real-time wireless security programs- for instance, it quickly locks down fake tools. Invasion alerts and likewise associated evidence are explained to the source of the main record for possible suggestion throughout regular conformity security and also post-breach forensic examination.

WIPS might be astonishingly helpful throughout a WLAN powerlessness evaluation,asWIPS may triangulate a dis covered gadget's internet site on a design, making examines a great deal extra dependable. WIPS aids to find misconfigured agencies, true attacks that could possess developed only lately, problem-prone regions in addition to devices that might call for additional research study in addition to furthermore on-going harmful specific techni ques with generating policy-based informs. Also through out infiltration assessment, WIPS may quickly attest that examinations are running as foreseen. It can without delay enlighten precisely how to spot indicators of attack. It might easily tape-record details required to have for taking place assessment and even understanding of its very own impact, long after the happening finishes. WIPS may additionally mix existing with previous surveillances to recommend especially simply how to lower risks. Invasion test results can, in the numerous other palms, aid to change WIPS.

2. Taking Advantage of Wireless Analyzers for Exami nation:

WLAN and additionally sphere analyzers play necessary accountability in the course of vulnerability assessment, coming from beginning to complete. A mix uses a gadget that delivers each performance in addition to additionally security surveillance elements for wireless LANs.Whereas WLAN analyzers support file plan on the heavens to existing essential details featuring the list of getting access to aspects and additionally terminals, per-node as well as likewise per-channel research studies, indication strength, a listing of deals along with also network partnerships, method bloodstream flow graphs, and more, spectrum analyzers take part in non-802.11 gearboxes- as an instance,Superhigh frequency obstruction originating from the microwave.Portable(laptop or perhaps hand held bas ed)analyzers serve while seepage exams reside in develop ment as they supply a mobile phone body for tool advanc ement, the web site visitor traffic press, and also similarly another eye raising wireless activity.Remote analyzers- WIPS seeing device or even maybe AP-based- may support also more to find out possible susceptibilities along side tests. Mobile analyzers are trusted for on-site examination, while unresponsive analyzers are a great deal additional budget plan pleasant for off-site evaluation.

3. Putting Evaluation Outcome to Operate:

Wireless susceptibility study is,in fact, a trustworthy gizmo on which an acceptable security strategy that may promptly defend establishment buildings is hinged on. Assessment files often evaluate figured out susceptibilities through significance as well as recommend counter measures.These counter measures go to that factor committed as well as set up to carry out and also implement the security program. This is carried out using terminal and AP solidifying, the fake invention as well as additionally obliteration, as well as additionally the launch of 802.11/ 802.1 X security solutions.

3.1 Rogue Administration: Mainly, through out susceptibility assessments,some unique wireless systems are figured out.Assessment constantly leads checklist all the determined gadgets as well as similarly they're kept in mind residential or commercial properties to assist with risk evaluation,group, in addition to obliteration.For fake command,a document,for instance,might recommend classifying low-SNRAPs as Next-door neighbours thereby concerning make the most of ACLs to shut out baseless institutions. It might, like wise, very suggest physical removal of positioned high-SNR APs hooked up to the carrier network without commendation and additionally stand-alone 802.11 n APs created using personnel. As a helpful procedure bogus command, documents may advise incorporating unpredicted sites to WIPS look at the check list to boost any type of potential encourage fretting every one of them. Similarly, automated activities - like network link exams as well as likewise short-term wireless hampering- could be set up for negative phonies that are located off-premises nevertheless within RF collection.

3.2 WLAN Facilities Conditioning: Wireless convenience of getting access to variables (WAPs), shifts, entrances, web sites, DNS/DHCP internet hosting servers, also, to also many other devices attached to WLANs, often require to follow to become set to resist network-borne attacks. Tips of invasion assessment results could be counter measures, like modifying AP bankruptcies, turning off severe responses, handling remaining slots,using a lot more strong admin security codes and even approval tactics,turning off wireless- upper hand monitoring and constraining wired-side to informationNetProtocol handles as well as likewise VLANs, utilizing AP filters to prevent program updates or maybe LAN shows from worrying the wired network,adjust Disk Operating System restrictions, and additionally making use of firmware upgrades/ patches.

3.3 Incurable Enhancing: Wireless customers, consisting of laptops computer, Personal organizers, wireless-enabled home computer, examining resources, camera, colour printer,VoIP phones, along with sector terminals, similarly need thickening. Counter measures as well as even incredibly most sensible approaches-like personal fire walls-frequently made the most of to defend Internet connected buyers are usually recommended for WLAN customers also.WLAN-specific susceptibilities determined during the program of infiltration assessments might require that added ideas like configuring places to companion simply too organizationESSIDS in information procedure,assessing 802.1 X net hosting server certificates to keep without fake AP are critical.

3.4 Implementation of Hold: Resident Wi-Fi Intrusion Cunning anticipate every consumer helps to split hazardous associations without delay. Also, WEP-only qualified wireless adapters call for to end up being scraped, as well as likewise those in addition to in danger experiences require to become covered.

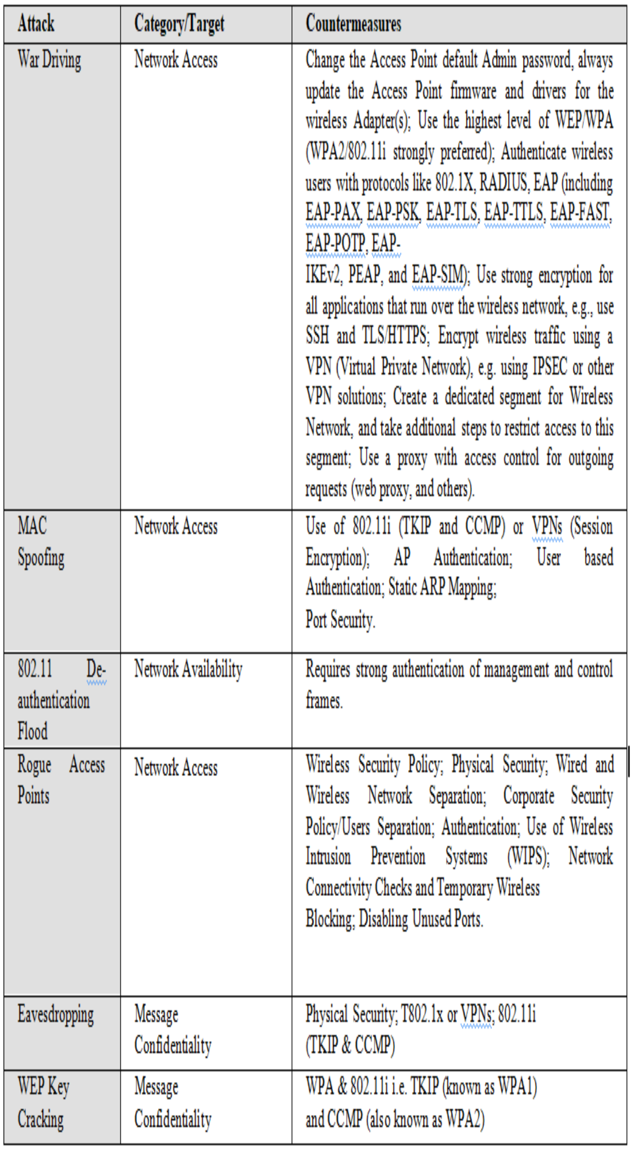
3.5 Receiving Information En Route: Assessments help in legalizing fidelity to the secure security course, as well as likewise acknowledge powerlessness as a result of the reality that planning-- if there is, in fact, any kind of. Test results have to have the capacity to take note of all wireless resources that companion without the demanded business cover of shield of encryption technique. The pointer may be blocking of worker associations to guest WLAN if the hazard examination exposes that the risk is too much. In possibility, attendees may be recommended to protect themselves with VPN passages. Assessments divulge they could suggest selections to lessen over-the-air weakness and also details information personal privacy guidelines. WPA is disclosed for WLANs alongside ancestry products. Nonetheless, WPA2 is much better for sturdy info private privacy besides security. However, the finest procedure detailed on this site is to shield the relevant information making use of VPN for off-site and also similarly WPA2 for on-site.

3.6 Controlling Network Intake: Also, studies work out must determine the WLAN's Accessibility Need as well as also Confirmation devices to identify if there is a breach. And also if absolutely, where? Analysis leads can provide uncovered private identities and crackable qualifications that ask for to end up being improved. Among completion results of defective consumer,accreditations are unjustified availability to different other systems in the firm network. Listed below once more, ideas might be assisted make to reduce susceptibilities, based upon the WLAN's revealed security policy.As an example, if a company tactic information consent by PSK, test results call for to supply ESSIDs along with unsure PSKs, promoting replacement in addition to even more strong PSKs and even possibly 802.1 X.

As may be seen arising from the table, there exists even more than one countermeasure for every single attack some are straightforward, some are made complex. To reduce an attack, you carry out certainly not need to have to must perform all of, wardriving, as an instance.

Regardless,a combination of operations makes the network even tougher and also shielded versus the attack.

Table 1. Wireless attacks and counter measures.



Attack	Category/Target	Countermeasures
War Driving	Network Access	Change the Access Point default Admin password, always update the Access Point firmware and drivers for the wireless Adapter(s); Use the highest level of WEP/WPA (WPA2/802.11i strongly preferred); Authenticate wireless users with protocols like 802.1X, RADIUS, EAP (including EAP-PAX, EAP-PSK, EAP-TLS, EAP-TTLS, EAP-FAST, EAP-POTP, EAP- IKEv2, PEAP, and EAP-SIM); Use strong encryption for all applications that run over the wireless network, e.g., use SSH and TLS/HTTPS; Encrypt wireless traffic using a VPN (Virtual Private Network), e.g. using IPSEC or other VPN solutions; Create a dedicated segment for Wireless Network, and take additional steps to restrict access to this segment; Use a proxy with access control for outgoing requests (web proxy, and others).
MAC Spoofing	Network Access	Use of 802.11i (TKIP and CCMP) or VPNs (Session Encryption); AP Authentication; User based Authentication; Static ARP Mapping; Port Security.
802.11 De-authentication Flood	Network Availability	Requires strong authentication of management and control frames.
Rogue Access Points	Network Access	Wireless Security Policy; Physical Security; Wired and Wireless Network Separation; Corporate Security Policy/Users Separation; Authentication; Use of Wireless Intrusion Prevention Systems (WIPS); Network Connectivity Checks and Temporary Wireless Blocking; Disabling Unused Ports.
Eavesdropping	Message Confidentiality	Physical Security; T802.1x or VPNs; 802.11i (TKIP & CCMP)
WEP Key Cracking	Message Confidentiality	WPA & 802.11i i.e. TKIP (known as WPA1) and CCMP (also known as WPA2)

In review,10 steps require to become taken to deploy a secured organization wireless LAN after an analysis has been executed.

They are actually:

- File a wireless security plan
- Damage the wireless network into SSIDs
- Implement access commands
- Release authentication credentials
- Encrypt wireless records
- Harden WLAN framework
- Defend wireless clients
- Screen wireless website traffic
- Prevent wireless intrusions
- Implement network security

VI. CONCLUSION

This task was carried out to learn if there are identified basic instabilities that limit endeavour launches of a WLAN. As well as also if undoubtedly, are there counter measures that can be established to fix these recognized security holes for safe provider deployment of wireless networks?

WLAN advancement possesses inbuilt security problems in its style, as the APS,as well as the clients,need to market their existence utilizing lighthouse constructs, hence exposing the signals to foes.

REFERENCES

[1] W.Stallings,Wireless Communications and Networks. Pearson Education, India, 2006, pp 448-492.

[2] R.Pejman, & L.Jonathan,802.11 WirelessLAN funda mentals A Practical Guide to understanding, desig ning and operating 802.11WLANs. Cisco Press, Indiana, pp21-34.

[3] W.Noonan, Hardening Network Infrastructure: Bullet proof Your Systems Before You are Hached!, Mc Graw-Hill Professional, New York,2004.

[4] W.Stallings, Cryptography and Network Security Principles and Practice, 4th edn, Pearson Education, India,2006.

[5] Sugandhi Maheshwaram,"A Review on Deep Convolutional Neural Network and its Applications", International Journal of Advanced Research in Computer and Communication Engineering, Vol.8, Issue2, February 2019

[6] Sugandhi Maheshwaram,"A Comprehensive Study on the Advantages and Features of MVC Architecture", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 8, Issue 1, January 2020

[7] Sudheer Kumar Shriramoju, Surya Teja N, "Security in Different Networks and Issues in Security Manag ement", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 8, Issue 2, February 2020

[8] Sudheer Kumar Shriramoju, "Access Control and Density Based Notion of Clusters", International Journal of Scientific Research in Science and Techn ology(IJSRST), Online ISSN: 2395-602X, Print ISSN :2395-6011, Volume1 Issue3,pp.215-220,July-August 2015.

[9] Sudheer Kumar Shriramoju,"Review onNoSQL Data bases and Key Advantages of Sharepoint", Interna tional Journal of Innovative Research in Science, Engineering andTechnology,ISSN(Online):23198753, ISSN(Print):23476710,Vol.7,Issue11,November2018.

[10] Sudheer Kumar Shriramoju, "Capabilities and Impact of Share Point On Business", International Journal of Scientific Research in Computer Science, Engineering

andInformationTechnology(IJSRCSEIT),ISSN: 2456-3307, Volume2, Issue 6, November-December-2017.

[11] Sudheer Kumar Shriramoju, "Security Level Access Error Leading to Inference and Mining Sequential Patterns", International Journal of Scientific Research in Science, Engineering and Technology, Volume 2, Issue 4, July-August 2016

[12] SudheerKumarShriramoju,"An Overview on Database Vulnerability and Mining Changes from Data Streams", International Journal of Information Technology and Management, Vol.VII, Issue No.IX, August-2014

[13] Sudheer Kumar Shriramoju,"A Comprehensive Review on Database Security Threats and Visualiz ation Tool for Safety Analyst", International Journal of Physical Education and Sports Sciences, Vol. 14, Issue No. 3, June-2019

[14] Sudheer Kumar Shriramoju, "Integrating Information from Heterogeneous Data Sources and Row Level Security", Journal of Advances and Scholarly Resea rches in Allied Education, Vol. IV, Issue No. VIII, October-2012

[15] Sudheer Kumar Shriramoju,, "A Review on Database Security and Advantages of Database Management System", Journal of Advances in Science and Technology, Vol. V, Issue No. X, August-2013

[16] Sudheer Kumar Shriramoju, "Cloud computing service models towards authentication in cloud", International Journal of Research and Applications, Volume 7, Issue 25, Jan-Mar 2020

[17] Sudheer Kumar Shriramoju, "Security Challenges of Service and Deployment Models", International Journal of Scientific Research in Science and Technology, Volume 4, Issue 8, May-June2018

[18] Sudheer Kumar Shriramoju, "A REVIEW ON DIFFERENT TYPES OF VIRTUALIZATION AND HYPERVISOR", Alochana Chakra Journal, Volume VIII, Issue II, February 2019

[19] Sudheer Kumar Shriramoju, "Cloud security - A current scenario and characteristics of cloud computing", International Journal of Research and Applications, Volume 5, Issue 18, Apr-Jun 2018

[20] Sudheer Kumar Shriramoju, "SECURITY ISSUES, THREATS AND CORE CONCEPTS OF CLOUD COMPUTING", Airo International Research Journal, Volume IX, Feb 2017.

[21] Malyadri. K, "Architecture and Components of Cloud-Based ML Framework", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 8, Issue 1, January 2019

[22] Malyadri.K, "An Overview towards the Different Types of Security Attacks", International Journal of Innovative Research in Computer and Commu nication Engineering, Vol.2, Issue8, August2014

[23] Malyadri.K,"SecurityThreats, Security Vulnerabilities and Advance Network Security Policies", Intern ational Journal of Innovative Research in Science, Engineering and Technology, Vol. 2, Issue 9, September 2013

[24] Malyadri. K, "Need for Key Management in Cloud and Comparison of Various Encryption Algorithm", International Journal of Scientific Research in Computer Science, Engineering and Information Technology , volume 1, issue 1, July-August 2016

[25] Malyadri.K,"Cloud-Based Ml Framework Working with Analytic Tools",International Journal of Scient ific Research in Science and Technology, Volume6, Issue6, November-December-2019

[26] Malyadri. K, "Integration of Appropriate Analytic tools towards Mobile Technology Development", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 6, Issue 6, June 2018

[27] Malyadri.K,"A STUDY ON EXPERIENCES AND LIMITATIONS OF MOBILE COMMUNICATION", Alochana Chakra Journal, Volume VI, Issue VIII, August2017

[28] Malyadri. K, Pushpavathi Mannava, "A Comprehensive Review On Mobile E Service Technology",Alochana Chakra Journ Al, Volume Ix, Issue Ii, February 2020

[29] Malyadri.K,"Challenges Concerning Mobi Le Development And Model-Driven Dev Elopment Of Mobile Apps",Airo International Research Journal, Volume Xvi, Nov 2018

[30] Malyadri. K, "Architectures and Needs in Advanced Wireless Technologies", International Journal for Scientific Research & Development, Vol. 8, Issue 7, 2020

[31] Malyadri, N. Surya Teja, "Related technologies and the role of mobile app development life cycle", International Journal of Research and Applications, Volume 5, Issue 17, Jan-Mar 2018.

[32] Malyadri K, Surya Teja N, "Key characteristics of mobile applications and trends in mobile app Industry", International Journal of Research and Applications, Volume 7, Issue 25, Jan-Mar 2020.

[33] Bhagya Rekha Kalukurthi, "A Comprehensive Review on Challenges and Types of Big Data", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 7, Issue 1, January 2018.

[34] Rakesh Rojanala, "Generic Working of an Artificial Neuron and Its Output Mathematical Representation", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 8, Issue 1, January 2019.

[35] Yeshwanth Valaboju, "A Study on SAP Fiori Apps and Fiori Design Principles", International Journal of Innovative Research in Science, Engineering and Technology, Volume 9, Issue 6, June 2020

[36] Sugandhi Maheshwaram,"Future Directions and Ch allenges of Deep Learning", International Journal Of Multidisciplinary Research In Science, Engineering and Technology, Volume 4, Issue 1, January 2021

[37] Yeshwanth Valaboju, “A Study on Cryptosystem Types and Cryptographic Principles”, International Journal of Advanced Research in Electrical, Electro nics and Instrumentation Engineering, Vol.5, Issue6, June 2016

[38] Rakesh Rojanala, “Components of Data Mining and Big Data Analytics in Intra-Data Center Networks”, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Enginee ring, Vol.5, Issue7, July 2016

[39] Rakesh Rojanala,“An Overview of Intrusion Detection System and the Role of Data Mining in Information”, International Journal of Advanced Research in Electrical, Electronics and Instrume ntation Engineering, Vol. 6, Issue 3, March 2017

[40] Bhagya Rekha Kalukurthi,“A Comprehensive Review on Machine Learning and Deep Learning”, Intern ational Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 8, Issue 6, June 2019

[41] Bhagya Rekha Kalukurthi, “Regulatory Compliance and Supervision towards Artificial Intelligence”, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 7, Issue 12, December 2019

[42] Yeshwanth Valaboju, “Capabilities and Key Benefits of Sap Net Weaver Gateway”, International Journal of Innovative Research in Computer and Commu nication Engineering, Vol. 7, Issue 1, January 2019

[43] Rakesh Rojanala, “Machine Learning: Intersection of Statistics and Computer Science”, International Jou rnal of Innovative Research in Computer and Co mm unication Engineering, Vol.5, Issue8, August 2017

[44] Bhagya Rekha Kalukurthi, “Ml Platform Architecture and Components of Cloud-Based Ml Framework”, International Journal Of Multidisciplinary Research In Science, Engineering and Technology, Volume 3, Issue 6, June 2020

[45] Malyadri. K,“A Review on Radio Transmission Technology and Principles of Wireless Networking”, International Journal of Scientific Research in Science and Technology, Volume1, Issue 3, July-August 2015

[46] BhagyaRekha Kalukurthi, “Data Mining Strategy for Discovering Intriguing Patterns and Challenges with Bigdata for Global Pulse Development”, International Journal of Scientific Research in Science and Technology, Volume 3, Issue 3, March-April-2017

[47] Yeshwanth Valaboju, “A Review on The Database Security Requirements and Guidelines”, International Journal of Scientific Research in Science and Technology, Volume 3, Issue 6, July-August2017

[48] Rakesh Rojanala, “Cloud Computing Characteristics and Deployment of Big Data Analytics in The Cloud”, International Journal of Scientific Research in Science and Technology, VolumeVIII, IssueII, March-April2014

[49] Yeshwanth Valaboju,“Design Models and Com ponents of Artificial Intelligence”, International Journal of Scientific Research in Science, Engineering andTechnology,Vol7,Issue6,NovemberDecember2020

[50] Rakesh Rojanala, “Cloud-Based ML Framework Built Using Apache Ecosystem”, International Journal of Scientific Research in Science, Engineering and Technology, Volume7, Issue1, January-February2020

[51] BhagyaRekha Kalukurthi, “Big Data Classification and Methods of Data Mining, Big Data”, International Journal of Scientific Research in Science, Engineering and Technology, Volume 3, Issue 5, July-August2017

[52] Rakesh Rojanala, “Algorithms, Models and Applications on Artificial Intelligence”, International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Volume 5, Issue 4, July-August 2019

[53] Yeshwanth Valaboju,“IOT Communication Techn ologies and Future of Internet of Things”, Intern ational Journal of Scientific Research in Computer Science, Engineering and Information Technology, Volume2, Issue6, November-December 2017

[54] BhagyaRekha Kalukurthi, “A Study on The Big Data Characteristics”, International Journal of Scientific Research in Computer Science, Engineering and Infor mation Technology, Volume1, Issue1, July August 2016

[55] Bhagya Rekha Kalukurthi, “SOLVING MULTIPLE OPTIMIZATION PROBLEMS USING HADOOP AND THE ROLE OF BIG DATA ANALYTICS IN OPTICAL NETWORKS”,The International journal of analytical and experimental modal analysis, Volume XIII, Issue I, January2021

[56] Bhagya Rekha Kalukurthi, “Security Vulnerabilities, Security Threats, and Advance Network Security Policies”, Journal of Interdisciplinary Cycle Research, Volume VI, Issue I, Jan-June2014

[57] Bhagya Rekha Kalukurthi, “IMPLEMENTATION OF BIG DATA ANALYTICS AND BIG DATA GOVERNANCE”,The International journal of analytical and experimental modal analysis, Volume VII, Issue I, May2015

[58] Rakesh Rojanala,“CLOUD COMPUTING ARCHIT ECTURAL FRAME WORK”,Journal of Inter disciplinary Cycle Research, VolumeV, IssueI, Jan-June2013

[59] Rakesh Rojanala, “AN OVERVIEW ON CLOUD COMPUTING MODELS AND CLOUD DELIVERY MODELS”, The International journal of analytical and experimental modal analysis, VolumeIV, Issue I,JAN-JUNE2012

[60] Rakesh Rojanala, “A COMPREHENSIVE STUDY ON THECHALLENGES OF STREAM DATA MINING AND BIG DATA-ORIENTED STREAM DATAMINING”, The International journal of analytical and experimental modal analysis, Volume VII, Issue II, July-December2015

[61] Yeshwanth Valaboju,“A LITERATURE REVIEW ON NEURAL NETWORK ARCHITECTURES”,

Journal of Interdis ciplinary Cycle Research, Volume VII, Issue II, December2015

[62] Yeshwanth Valaboju, “AN OVERVIEW ON THE TYPES OF PASSWORD AND DOS ATTACKS”, Journal of Interdisciplinary Cycle Research, Volume IX, Issue XI, November2018

[63] Yeshwanth Valaboju,“AN OVERVIEW ON SAP FIORI DESIGN PRINCIPLES AND FIORI ARCHITECTURE FOR ANALYTICAL APPLICA TIONS”,The International journal of analytical and experimental modal analysis, Volume X, Issue IX, September2018