International Journal of Scientific Research & Engineering Trends
Volume 7, Issue 1, Jan-Feb-2021, ISSN (Online): 2395-566X

A Comprehensive Overview of WLAN Security Attacks

Yeshwanth Valaboju
Technical Manager
Rigved Technologies Pvt. Ltd, India

***Abstract*- Wireless communication has broken the constraint individuals utilized to have also in addition to wired innovation. The right to gain access to provider network without being bound, versatility while accessing the Internet, boosted consistency, as well as adaptability, are an amount of the variables steering the wireless LAN modern-day technology. Different other variables that contribute to the impressive development of Wireless Area Networks(WLANs) are lessened setup time, enduring cost discount rates, and likewise instalment in difficult-to-wire areas. Wireless LANs level of popularity has performed the growth as a result of the fostering of the IEEE 802.11 b spec in 1999. Over the last couple of years, wireless LANs are widely set up in a location like company, federal authorities bodies, health care centres, colleges and also building atmosphere.**

***Keywords*- Threats, vulner abilities, security attacks.**

I.INTRODUCTION

Today, Wireless Lan(WLAN) is a collection to reckon in numerous markets, including company, education and learning and learning, authorizations, social as well as particular.IEEE802.11 controls wireless media innovation. This may be accepted to the cheap of the equipment as well as likewise much higher records expenses that aid present uses (coming from 1 to 54 Mbps) along side stimu lating potential extensions (likely discussing one hundred Mbps with 802.11n). Considerably, mobile phone systems (Laptop, Personal Organizers, and like wise Tablet PCs) are being industries along with wireless LAN as a necessary component.

However, this innovation brings together with its critical restrictions in the business of security.The communication device of the wireless LAN is a frequency wave. Consequently, it is added in danger to eavesdropping than wired networks, as well as likewise as the wireless market rises, the security concerns develop along with it. There has been a lot handle WLAN security, thinking about that it was learnt that the 802.11 security type is unsteady. Nonetheless, most of these jobs got on the security unit enlargement. For a company to perfect guard its info,there is a necessity for security threat examination. This will certainly help to determine the threats its info is prone to, and also afterwards generate effective security activities to avoid it.

Wireless local area network (WLANs) synchronize as the common LAN, but they have a wireless user interface, for that reason offering location-independent network access. It permits a close-by network of computers to switch info or may be some other relevant information through electro magnetic radiation along with without utilizing cable television service. It can easily either alternative or, much more often, increase a wired LAN. Today, wireless LANs have occupied a significant sector in the lan market. Considerably,providers have found out that wireless LANs are real accessory to traditional wired LANs, to thrill the needs for action, moving, unscripted networking, as well as also insurance coverage of areas harsh to cable television.

This phase supplies a quick questionnaire of wireless LANs. The adhering to subtopics were dealt with: nece ssary WLAN parts, WLAN transmission modern inno vation, WLAN range allowance, WLAN locations and also WLAN applications.

II. BASIC WLAN COMPONENTS

For one to develop a wireless computer network,2 easy elements should be readily accessible: wireless network sd card, along with wireless, acquire access to point(s). The 3rd crucial component, wireless hyperlink, is made use of to hook up a pair of or even additional properties.

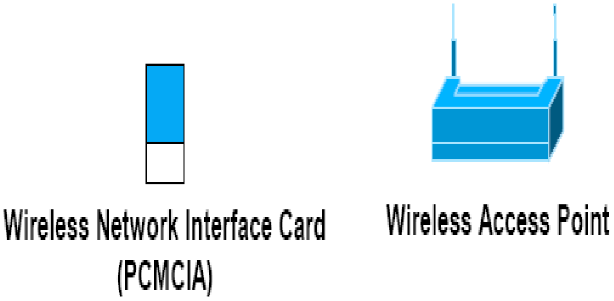

Fig 1. Basic components of WLAN.

The wireless network flash memory card is attached to the mobile phone computer, as well as they connect to an access variable. An availability part is virtually a centre that supplies wireless customers with the capability to attach to the wired LAN basis. To sustain a coverage location, greater than one obtains access to factors are utilized as in cell constructs, which are made use of by cellphone suppliers to insist on a protected area. Wireless hyperlinks, however, allow high-speed lengthy variation outdoor links in between residential or commercial properties. Based upon line-of-sight, wireless bridges are not impacted via hurdles consisting of free ways, railways, and physical bodies of water, which usually pose a problem for copper as well as the fibre-optic wire.

III. THREATS AND VULNER ABILITIES

Figure2 gives a key taxonomy of security assaults to assist companies and likewise, individuals understand many of the attacks against WLANs.

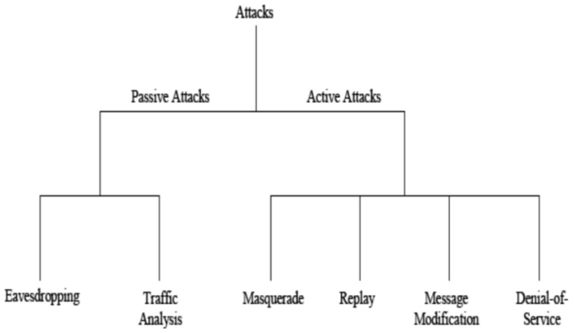

Fig 2. Taxonomy of Security Attacks.

Network security strikes are normally separated into passive in addition to spirited strikes.These two extensive training class are afterwards partitioned right into several other sorts of assaults.

1.Stationary Spell: A strike where an unauthorized festivity get to a source along with carries out undobtedly not fine-tune its info (i.e., eavesdropping). Easy spells might be either eavesdropping and even web site traffic analysis (in some cases described as visitor traffic flow research study). These pair of effortless spells are defined listed below.

- **Eavesdropping:** The assailant observes broadcasts for notice web content. An instance of the particular assault is a private hearing near right into the broad casts on a LAN between pair of work stations and even adjusting into delivering in between a wireless mobile phone and also a base station.
- **Web Visitor Traffic Assessment:** The challenger, in an extra understated way, boosts notification through keeping an eye on the programs for designs of communication. A substantial volume of infor mation it had in the blood circulation of alerts in between hooking up occasions.

2. Active Strike: A strike whereby an unjustified event generates adjustments to a notification, files circulation, or perhaps papers. It is possible to find this sort of strike, however, it could not be possible to avoid. Energetic assaults could take the type of some of 4 types: Masquerading, Replay, Information modification, and also Denial-Of-Service(Disk Operating System).These attacks are identified listed here.

2.1 Posing: The enemy impersonates a professional customer and likewise there using boosts specific ungrounded options.

2.2 Replay: The opponent checks transmissions(passive assault) and also retransmits relevant infor mation as the official consumer.

2.3 Notice Modification: The aggressor changes valid relevant information by erasing, adding to, modif ying, or even reordering it.

2.4 Denial-Of-Service: The foe prevents or even dis allows the common consumption and even moni toring of interactions sources.

The risks linked with 802.11 are the outcome of several of these strikes.The consequences of these attacks consist of, having said that, are certainly not limited to, reduction of exclusive details, lawful as well as rehabilitation expenses, stained image, and also the reduction of network service. As the lot of associations that set up wireless networks remains to increase, it finds yourself being a great deal a lot more essential to understand the types of susceptibilities as well as likewise threats coming across tradition IEEE 802.11 WLANs and apply ideal security services. Numerous of the weakness that is illustrated is belonging to the legacy IEEE802.11 WLAN standard, while others connect to WLANs or wireless social network normally.

3. Loss of Prudence:

Because of the system and also broadcast characteristic of wireless modern technology, making certain discern ment is substantially more difficult in a wireless network than a wired network. Criterion wired networks provide fundamental security via using a physical tool to which an aggressor needs to gain access to. Wireless networks multiply signs into the room, developing typical physical security countermeasures less reputable along with accessibility to the system a great deal easier,boosting the importance of ample discernment on wireless networks.

Static eavesdropping on heritage IEEE 802.11 WLAN interactions might induce significant threat to a firm. An opponent can easily check Superhigh frequency signals as well as additionally take hold of data going across the wireless resource. At- risk info, featuring unique inform ation, network I.d.s and codes, as well as even put to gether documents, are some occasions of info that could be grabbed. In addition to that, aggressors along with high-gain aerials might record documents arising from wireless networks past a network's normal operating variation, once again developing discretion a crucial security action.

Eavesdropping executed with a wireless network analyzer information or even sniffer is incredibly quick as well as quick and easy for heritage IEEE 802.11 WLANs.Noes may make use of issues in the key scheduling formula that was given the completion of RC4 used using WEP. To take advantage of these weak spots, the nose passively keeps an eye on the WLAN and also finds out the security techniques after a changeable volume of packages has been scented. On a saturated network, picking up the volume of relevant information demanded to determine theWEP tricks just takes lots of hrs; if web site web traffic quantity is decreased, it might use up to eventually. For instance, a busy AP that is moving3,000 bytes at 11Mbps is going to run through the 24-bit IV space after roughly 10 hrs. As quickly as the aggressor recovers 2 cypher messages that have used the same IV, both files sincerity, as well as discernment, might be run the risk of.

Yet another risk to WLANs is the decrease of prudence with straightforward eavesdropping on course internet traffic. Ethernet centres usually relay network internet visitor traffic to all physical user interfaces and also hooked up gizmos, which leaves the relayed guest traffic vulnerable to unauthorized monitoring. As an example, an AP connected to a port on an Ethernet centre that is broadcasting reports website visitor traffic would divulge every one of the documents markets it jumped on its wired interface over its wireless user interface. Making use of the Ethernet hub structure boosts the danger that the AP could be communicating full or even vulnerable relevant information that was transmitted along with the hub. Switches ease this stress by offering focused networks between communication devices.

A dangerous or even irresponsible individual may surreptitiously practically place a bogus AP into a storage room, under a meeting rooms table, or in every other shock place within a framework.The rogue AP might then be made use of to enable uncalled-for individuals to access to an organization network. Such a long time as its site remains near the consumers of the WLAN,and also it is put together to look like a legitimate AP to wireless customers, the rogue AP may effectively lure wireless clients of its validity and also cause wireless customers to hyperlink as well as transmit website visitor traffic to the artificial AP.

Within this situation, an assaulter can very easily capture each one of the files sent out via the fake AP, bypassing all wireless procedure discretion. It is additionally vital to bear in mind that certainly not all rogue Aps are discharged using detrimental individuals. Often, rogue APs are set up by customers that desire to take advantage of wireless modern technology without the confirmation of the IT department. These APs are commonly put together without efficient security setups and also position significant security threats.

4. Decrease of Credibility:

Records honesty troublesin wireless networks correspond to those in wired networks. Because affiliations consistently perform wireless and wired interactions without sufficient cryptographic protection of reports, reliability might be challenging to complete. As an example, an aggressor may endanger documents honesty via eliminating or even individualizing the info rmation in an e-mail with the wireless unit. This may be destructive to an institution if the required email is commonly distributed amongst email recipients because the security features of the tradition IEEE802.11 standard does certainly not deliver stringent notification integrity, different other kinds of active spells that jeopardize device credibility is viable.

5. Loss of Book:

A denial of WLAN source generally involves some form of DoS spell, like playing or even flooding. Sticking establishes when an RF sign given off from a wireless unit bewilders other wireless tools and also indications, triggering a decline of interactions.Clogging may be caused especially through a detrimental consumer or started accidentally via ejections from additional trust worthy units managing within the illegal array, including a cord-less telephone or perhaps microwave. Flooding strikes are started using program request brought in to move a wide range of packages to an AP or various other wireless gadgets, triggering the unit to end up being baffled through packages and end common procedure. Flooding can set off a WLAN to malfunction to an incorrect functions level or even maybe stop working altogether. Adhering in addition to overloading risks, are challenging to resist in any kind of radio-based communications, and also the practice IEEE 802.11 requirements carries out not give any kind of defence against each of all of them.

IEEE 802.11 control frameworks offer one more angle for DoS strikes against WLANs. Keeping an eye on structures control the strategy of linking and also dis affiliating APs in addition to STAs coming from a WLAN. Intentionally, the IEEE 802.11 requirement carries out not to supply security against these strikes. If an adversary creates a disassociation building as well as delivers it to an AP or even STA, the targeted gizmo will undeniably grant the demand and likewise shut its very own communications affiliation. Another type of assault, described as an association assault, targets an AP's association table, which tracks the disorder of STAs related to the AP.An organization usually assault floodings this table along with misleading requests until the AP no longer permits genuine institutions. Advanced affiliation spells might drive STAs to attach to sneaky APs where the patient goes through a wide variety of harmful strikes.

Consumers can easily also cause a loss of vacancy by unexpectedly monopolizing the capacity of a WLAN, including installing major files, successfully denying numerous other individuals access to the network.

IV. WLAN SECURITY ATTACKS

Often, security troubles in the WLAN world are sorted right in to physical besides rational.There are many security threats and additionally attacks that can conveniently injure the security of WLANs.Those attacks may be realized right into practical attacks and also physical attacks.

1. Reasonable Attacks:

1.1 MAC COMPUTER PC UNIT Care For Spoofing:

MACINTOSH COMPUTER deals with are delivered in the clear when communication in between STAs as well as also AP happens. A strategy to defend availability to APs and also as a result of this to the network is accomplished to refuse several other buyers coming from paying attention to the communication. Integrity suggests always keeping the accurateness in addition to the rule of particulars transmitted in between STAs and also AP. Any form of a security solution must obtain this 3 target at in addition to one another

The security, as well as also management concern, happened big as far more APs,are mounted in the network. Thereby there is a demand to validate and likewise deal with security concerns in a few WLANs besides significant ones in addition to a requirement to generate strategies to stand up to security risks. As WLANs treatments like wireless World wide web and also wireless eCommerce dispersing swiftly, there is a need to make certain the security of such therapies.

1.2 Attacks on WEP:

Wired Matching Individual Privacy(WEP) is a security protocol based on security formula gotten in touch with "RC4" that targets to pay for to the WLAN matching to the security provided in the wired LAN.WEP possesses bunches of downsides like the treatment of little Initialization Slant(IV) as well as further more brief RC4 security pointer as well as likewise taking advantage of XOR method to cypher the trick with the plain text to create cipher text notification. Delivering the Macintosh Personal Computer Desktop Computer deals with in addition to also the IV in the clear in addition to the repeating utilization a single IV and also the fact that covered secrets are cooperated in between interactions celebrations are WEPs considerable security problems.

1.3 Rejection Of Service Attack: Denial of Service attacks or DoS is a severe risk on each wired and also wireless networks. This attack strives to disable the supply of the system alongside the business it offers. In WLANs, DoS is carried out in a bunch of procedures like distinguishing the harmony selection through outdoors Radio Frequency sources, for that reason, denying access to the WLAN and also,in straight-out suitable events, supplying acquire access to together with lessened files expenses.

1.4 Man-In-The-Middle Attack:

This is a prominent attack in both wired and also wireless networks. An unapproved STA obstructs the interaction between real STAs and likewise the AP. The forbidden STA blockheads the AP and also conditions to end up being a reliable STA; meanwhile, it additionally block heads the opposite STA as well as additionally proclaims to find your self being relied on AP. Fig3 set Man-in Middle attack

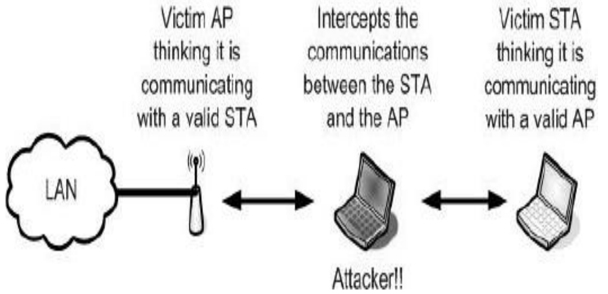
Victim AP thinking it is communicating with a valid STA
Intercepts the communications between the STA and the AP
Victim STA thinking it is communicating with a valid AP
LAN
Attacker!!

Fig 3. Representation of Man-in-Middle Attack.

1.5 Poor Network-Style:

WLANs operate as an advancement to the wired LAN. As a result, the security of the LAN depends really on the protection of the WLAN.The vulnerable point of WLANs means that the wiredLAN degrees on danger.A dependable WLAN style requires to have to end up being utilized using making an effort to split up the WLAN coming from the wired LAN through placing the WLAN in the Demilitarized Zone(DMZ) alongside firewall plan software program, re modellings along with any sort of added reach manage technology to restrain the accessibility to the WLAN. I reside in add-on dedicating certain subnets for WLAN than the when utilized for wired LAN may help in preventing security transgressions. Mindful wired and also wireless LAN network-style participates in a required component to protect access to the WLAN.

1.6 Delinquency Ap Arrangements:

The majority of APs are supplied together with the minimum demanded and even no security agreement using insolvency. This keeps thinking of that providing them along with all security components made it possible for are heading to create consumption along with functionality made complex for regular customers.The functionality of AP merchants is actually to supply much higher facts cost, far from bundle setup APs without a truthful commitment to security. Network security managers need to configure these AP depending on the organization's security planning. Several of the default unsafe settings in APs moved today are default codes which attack end up being unstable or even bare.

1.7 SSID:

Option Specify Identifier (SSID) is the label supplied a particulars WLAN, and also it is introduced as a result of the AP, the proficiency of SSID is needed as well as also operates as the very first security self-defence. Sadly, using misbehaviour, some APs shut down SSID demand which shows people may rapidly access the WLAN without confirming the skills of SSID. Meanwhile, some APs don't threaten SSID demand; in truth, the SSID demand is made it manageable for however, the SSID title by itself is advertised airborne. This is nevertheless an additional security issue as a result of the reality that it markets the lifestyle of the WLAN. SSID requirements need to have to be allowed in addition to SSID headlines shouldn't be announced; therefore, individuals need to provide the expertise of WLAN's SSID just before building communication.

2. Physical Attacks:

2.1 Rogue Obtain Access to Traits:

In day-to-day circumstances, AP accepts STAs to admit to the WLAN. The AP has never sought permission if the AP is placed without the IT facility's understanding. These APs are contacted "RogueAPs", and also they establish a secure space in the network. A foe can quickly put in a Rogue AP together with security capabilities damaged creating a mass security threat. There is a standard for reciprocal confirmation in between STAs along withAPs to ensure that each party are real. Network security managers might learn Phony APs by making use of wireless assessing resources to appear together with check out the network.

2.2 The Physical Positioning of Aps:

The setup place of APs is additional security trouble because positioning APs wrongly will subject it to physical attacks. Enemies may quickly modify the APs as soon as discovered causing theAP to turn to its vulner able bank ruptcy settings. It is quite vital for network security managers to the proper way to select dreamlands to install APs.

V. CONCLUSION

The key variables in between WLANs, as well as additionally wired/fixed LANs, is that WLANs counts on Superhigh frequency(Carrier frequency) signs as an interaction device. The indications relayed due to the AP might comfortably circulate outside the boundary of a region and even a design, where an AP is set up, allowing folks who are not in fact in the property to follow to the network. Attackers utilize unique tools and also scenting gizmos to locate simply available WLANs and also tune in on online communications while helping an auto mobile or perhaps strolling around. Since Carrier frequ ncy signs follow no restrictions, aggressors outside a building might get such indicators as well as also launch attacks on the WLAN. This sort of attack is referred to as "match driving". Openly quickly available resources are capitalized on for battle steering like Web Stumbler. Fanatics also chalk constructs to advise that red flags remain in reality transferred from the system, and additionally, the WLAN might be incredibly effortlessly accessed. This branding is also called"battle fluid chalking". In Fight fluid chalking, details regarding the rate of the relationship and also additionally whether the proof unit utilized is open or even shared secrets are suggested including unique codes embedded in between war-chalkers.

REFERENCES

[1] Prof.SatishK.Shah,Ms.Sonal JRane,Ms. Dharmistha D. vishwakarma (2012)“Performance Evaluation of Wiredand Wireless Local Area Networks” Inter national Journal of Engineering. Research and Deve lopment

[2] Prof.Vilas Deotare,Sunil Wani,Swati Shelke (2014) “Wired Equivalent Security Algorithm for Wireless LAN”International Journal of Emerging Techn ology and Advanced Engineering.

[3] Sachi Pandey, Vibhore Tyagi (2013) “Performance Analysis of Wired and Wireless Network using NS2 Simulator”International Journal of Computer Applications.

[4] KarthikLakshminarayanan,VenkataN.Padmanabhan, Jitendra Padhye “Bandwidth Estimation in Broad band Access Networks”.

[5] AnthonyC.Ijeh,AllanJ.Brimicombe,DavidS.Preston, Chris.O. Imafidon “Security Measures in Wired and WirelessNetworks”

[6] Sugandhi Maheshwaram,“A Review on Deep Conv olutional Neural Network and its Applications”, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 8, Issue 2, February 2019

[7] Sugandhi Maheshwaram, “A Comprehensive Study on the Advantages and Features of MVC Architecture”, International Journal of Innovative Research in Computer and Communication Engin eering, Vol.8, Issue1, January 2020

[8] SugandhiMaheshwaram,“CLOUD DEPLOYMENT STRATEGIES AND CONCEPTUAL VIEW OF CLOUD COMPUTING”,Alochana Chakra Journal, Volume VIII, Issue VI, June2019

[9] SugandhiMaheshwaram,“A Comprehensive Review on the Implementation of Big Data Solut ions”, International Journal of Information Technology and Management Vol. XI, Issue No.XVII, November-2016,

[10] Sugandhi Maheshwaram,“Challenges of the Mobile Web for Development”, International Journal of Innovative Research in Science, Engineering and Technology, Volume 9, Issue 8, August 2020

[11] Sugandhi Maheshwaram,“A STUDY ON THE CHALLENGES IN HANDLING BIG DATA”,

International Journal of Research, VolumeVIII, IssueIII, March 2019

[12] Sugandhi Maheshwaram,“A Study On The Concept And Evolution Of Machine Learning”,International Journal For Research & Development In Techno Logy, Volume-11,Issue-5, May-19

[13] Sugandhi Maheshwaram, “A Novel Technique For Preventing The Sql Injection Vulnerabilities”, International Journal Of Research And Applications, Volume 5, Issue 19, July-Sep 2018

[14] Sugandhi Maheshwaram,“A Study On Security Information And Event Management (Siem)”, International Journal Of Research And Applications, Volume 5, Issue 17, Jan-Mar 2018

[15] Sugandhi Maheshwaram, “A Study Design Of Big Data By Concentrating On The Atmospheric Infor Mation Evaluation”, International Journal For Scientific Research & Development, Vol.7, Issue 03, 2019

[16] Sugandhi Maheshwaram,“Architectural Framework Of Cloud Computing Environment”, International Journal Of Scientific Research In Science, Enginee Ring And Technology, Volume4, Issue1, January-February2018

[17] Sugandhi Maheshwaram, “An Overview Of Open Research Issues In Big Data Analytics”, Journal Of Advances In Science And Technology, Vol. 14, Issue No. 2, September-2017

[18] Sugandhimaheshwaram,“Cloud Deployment Strategies And Conceptual View Of Cloud Computing”,Alochana Chakra Journal, Volume Viii, Issue Vi, June2019

[19] Sugandhimaheshwaram,“A Study On Vulner Abilities, Applications, Advantages And Routing Protocols In Manet”, International Journal Of Scientific Research In Science And Technology, Volume 4, Issue 1, January-February2018

[20] Sugandhi Maheshwaram, “An Overview Towards The Techniques Of Data Mining”, Research Review International Journal Of Multi Discipl Inary, Volume04, Issue02, February 2019

[21] Sudheer Kumar Shriramoju, Surya Teja N,“Security In Different Networks And Issues In Security Management”, International Journal Of Innovative Research In Computer And Communication Engineering, Vol.8, Issue2, February 2020

[22] Sudheer Kumar Shriramoju,"Access Control And Density Based Notion Of Clusters",International Journal Of Scientific Research In Science And Technology(Ijsrst),Onlineissn:2395602x,Printissn:2395-6011, Volume1 Issue3, Pp.215-220, July-August 2015.

[23] Sudheer Kumar Shriramoju, “Review On Nosql Databases And Key Advantages Of Sharepoint”, International Journal Of Innovative Research In Science, Engineering And Technology, Issn (Onl ine): 2319-8753, ISSN (Print): 2347-6710, Vol. 7, Issue 11, November 2018.

[24] Sudheer Kumar Shriramoju,“Capabilities and Impact of Share Point On Business”, International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSR CSEIT), ISSN:2456-3307, Volume2, Issue6, November-December-2017.

[25] 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

[26] Sudheer Kumar Shriramoju, “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

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

[28] Sudheer Kumar Shriramoju,“Integrating Inform ation from Heterogeneous Data Sources and Row Level Security”, Journal of Advances and Scholarly Researches in Allied Education, Vol. IV, Issue No. VIII, October-2012

[29] Sudheer Kumar Shriramoju,,“A Review on Data base Security and Advantages of Database Management System”,Journal of Advances in Science and Technology,Vol.V,IssueNo.X, August-2013

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

[31] 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

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

[33] 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

[34] Sudheer Kumar Shriramoju, “SECURITY ISSUES, THREATS AND CORE CONCEPTS OF CLOUD COMPUTING”, Airo International Research Jour nal, Volume IX, Feb 2017.

[35] 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

[36] Malyadri. K, “An Overview towards the Different Types of Security Attacks", International Journal of

Innovative Research in Computer and Commu nication Engineering, Vol.2, Issu 8, August 2014

[37] Malyadri.K, "Securit Threats, Security Vulner Abilities And Advance Network Security Policies", International Journal Of Innovative Research In Science, Engineering And Technology, Vol.2, Issue9, September 2013

[38] 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

[39] Malyadri. K,"Cloud-Based Ml Framework Working With Analytic Tools", International Journal Of Scientific Research In Science And Technology, Volume 6, Issue 6, November-December-2019

[40] 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

[41] Malyadri. K,"A Study On Experiences And Limitations Of Mobile Communica Tion", Alochana Chakra Journal, Volumevi, Issue Viii, August2017

[42] Malyadri.K,Pushpavathimannava,"A Compre Hensive Review On Mobile E-Service Technology",Alochana Chakra Journal, Volu Me Ix, Issue Ii, February 2020

[43] Malyadri.K,"Challenges Concerning Mobile Development And Model Driven Development Of Mobile Apps", Airo International Research Journal, Volume Xvi, Nov 2018

[44] Malyadri. K, "Architectures And Needs In Advanced Wireless Technologies", International Journal For Scientific Research & Development, Vol. 8, Issue 7, 2020

[45] 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.

[46] 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.

[47] 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.

[48] Rakesh Rojanala, "Generic Working Of An Artificial Neuron And Its Output Mathematical Represe Ntation", International Journal Of Innovative Research In Science, Engineering And Technology, Vol. 8, Issue 1, January 2019.

[49] 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

[50] Sugandhi Maheshwaram,"Future Directions and Challenges of Deep Learning",International Journal Of Multi disciplinary Research In Science, Engine ering and Technology, Volume 4, Issue 1, January 2021

[51] Yeshwanth Valaboju, "A Study on Cryptosystem Types and Cryptographic Principles", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 5, Issue 6, June 2016

[52] 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 Engine ering, Vol. 5, Issue 7, July 2016

[53] 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

[54] Bhagya Rekha Kalukurthi, "A Comprehensive Review on Machine Learning and Deep Learning", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engine ering, Vol.8, Issue 6, June 2019

[55] 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

[56] Yeshwanth Valaboju,"Capabilities and Key Benefits of Sap NetWeaver Gateway", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 7, Issue 1, January 2019

[57] Rakesh Rojanala, "Machine Learning: Intersection of Statistics and Computer Science", International Journal of Innovative Research in Computer and Communication Engineering, Vol.5, Issue8, August 2017

[58] Bhagya Rekha Kalukurthi,"Ml Platform Archit cture and Components of Cloud-Based Ml Frame work",International Journal Of Multi disciplinary Research In Science, Engineering and Technology, Volume 3, Issue 6, June 2020

[59] Malyadri. K,"A Review on Radio Transmission Technology and Principles of Wireless Netwo rking",International Journal of Scientific Research in Science and Technology, Volume1, Issue3, July-August 2015

[60] BhagyaRekha Kalukurthi, "Data Mining Strategy for Discovering Intriguing Patterns and Challenges with Bigdata for Global Pulse Development", Intern ational Journal of Scientific Research in Science and Technology, Volume3, Issue 3, March-April-2017

[61] Yeshwanth Valaboju, "A Review on The Database Security Requirements and Guidelines", Interna tional Journal of Scientific Research in Science and Technology, Volume 3, Issue 6, July-August2017

[62] Rakesh Rojanala,"Cloud Computing Characteristics and Deployment of Big Data Analytics in The Cloud", International Journal of Scientific Research in Science and Technology, Volume VIII, Issue II, March-April2014

[63] YeshwanthValaboju,"Design Models and Components of Artificial Intelligence",International Journal of Scientific Research in Science, Engin eering and Technology, Vol7, Issue6, November December 2020.

[64] Rakesh Rojanala,"Cloud-Based ML Frame work Built Using Apache Ecosystem",International Journal of Scientific Research in Science, Engine ering and Technology, Volume7, Issue1, January-February2020.

[65] Bhagya Rekha Kalukurthi, "Big Data Classification and Methods of Data Mining, Big Data", Interna tional Journal of Scientific Research in Science, Engineering and Technology, Volume3, Issue5, July-August2017

[66] Rakesh Rojanala,"Algorithms, Models and Applic ations on Artificial Intelligence", International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Volume 5, Issue 4, July-August 2019

[67] Yeshwanth Valaboju,"IOT Communication Techn logies and Future of Internet of Things", Intern ational Journal of Scientific Research in Computer Science, Engineering and Information Technology, Volume2, Issue6, NovemberDecember 2017

[68] Bhagya Rekha Kalukurthi,"A Study on The Big Data Characteristics",International Journal of Scientific Research in Computer Science, Engineering and Information Technology,Volume1, Issue1, July-August 2016

[69] 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

[70] Bhagya Rekha Kalukurthi, "Security Vulner abilities, Security Threats, and Advance Network Security Policies",Journal of Interdisciplinary Cycle Research, Volume VI, Issue I, Jan-June2014

[71] 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

[72] Rakesh Rojanala, "CLOUD COMPUTING ARCHI TECTURAL FRAMEWORK",Journal of Inter disciplinary Cycle Research, VolumeV, IssueI, Jan-June2013

[73] Rakesh Rojanala,"AN OVERVIEW ON CLOUD COMPUTING MODELS AND CLOUD DELI VERY MODELS", The International journal of analytical and experimental modal analysis, VolumeIV, Issue I,JAN-JUNE2012

[74] 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, Volu me VII, Issue II, July-December2015

[75] Yeshwanth Valaboju, "A LITERATURE REVIEW ON NEURAL NETWORK ARCHITECTURES", Journal of Inter disciplinary Cycle Research, Volume VII, Issue II, December2015

[76] Yeshwanth Valaboju, "AN OVERVIEW ON THE TYPES OF PASSWORD AND DOS ATTACKS", Journal of Inter disciplinary Cycle Research, Volume IX, Issue XI, November2018

[77] Yeshwanth Valaboju,"AN OVERVIEW ON SAP FIORI DESIGN PRINCIPLES AND FIORI ARCHITECTURE FOR ANALYTICAL APPLIC ATIONS",The International journal of analytical and experimental modal analysis, Volume X, Issue IX, September2018