JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

An Overview on the Taxonomy of Security Attacks

K. RamyaSri[1]

[1]Associate Consultant, Kotak Associates, Bangalore, India

ABSTRACT

For an organization to ideal guard its information, there is a need for security danger assessment. This will aid to identify the threats its info is prone to, and after that create proper security actions to resist it. Wireless communication has broken the constraint consumers made use of to have even along with wired innovation. The liberty to gain access to company network without being bonded, flexibility while accessing the Web, improved dependability and flexibility are a number of the factors steering the wireless local area network modern technology. Various other factors that add to the remarkable growth of Wireless Local Area Networks (WLANs) are lessened installation time, long-lasting price discounts, and also instalment in difficult-to-wire locations. Wireless LANs popularity has performed the rise because of the adoption of the IEEE 802.11 b specification in 1999.

Index Terms: threats, vulnerabilities, security attacks

I. INTRODUCTION

Today, Wireless Local Area Network (WLAN) is a selection to reckon in various markets, featuring business, education and learning, authorities, public and specific. IEEE 802.11 controls wireless media technology. This can be credited to the cheap of the hardware and also higher data fees that assist current applications (from 1 to 54 Mbps) along with encouraging future extensions (potentially going over one hundred Mbps with 802.11 n). Significantly, mobile units (Laptop computers, Personal Organizers, and also Tablet PCs) are being marketed with wireless LAN as an essential component.

However, this innovation brings along with its crucial limits in the field of security. The communication tool of the wireless LAN is a frequency wave. Therefore it is extra at risk to eavesdropping than wired networks, and also as the wireless market increases, the security issues grow alongside it. There has been much deal with WLAN security, considering that it was found out that the 802.11 security style is unstable. Nevertheless, most of these jobs got on the security device augmentation. Over the last few years, wireless LANs are extensively deployed in a location like business organizations, federal government bodies, healthcare facilities, colleges as well as even property environment. Movement, flexibility, scalability, cost-effectiveness and quick release are a few of the aspects driving the expansion of modern technology. This paper gives the representation of man-in-middle attack and WLAN security attacks.

Wireless computer network (WLANs) coincide as the typical LAN, but they have a wireless interface, therefore offering location-independent network accessibility. It permits a nearby network of computers to swap information or even other information by electromagnetic radiation as well as without using cable televisions. It can easily either substitute or, even more usually, expand a wired LAN. Today, wireless LANs have occupied a considerable segment in the local area network market. Considerably, companies have discovered that wireless LANs are real attachment to conventional wired LANs, to delight the needs for movement, moving, impromptu networking, and also insurance coverage of locations harsh to cable.

This phase supplies a quick survey of wireless LANs. The complying with subtopics were covered: essential WLAN components, WLAN transmission modern technology, WLAN spectrum allocation, WLAN geographies and also WLAN applications.

II. BASIC WLAN COMPONENTS

For one to establish a wireless local area network, two simple components should be readily available: wireless network memory cards, as well as wireless, get access to point(s). The third essential component, wireless link, is made use of to connect pair of or more buildings.

The wireless network memory cards are affixed to the mobile computer, as well as they link to an access factor. An accessibility aspect is practically a hub that provides wireless customers with the ability to affix to the wired LAN backbone. To maintain a coverage location, greater than one get access to factors are made use of as in cell constructs, which are used by cell phone providers to assert a protection region. Wireless links, on the contrary, permit high-speed long- variation exterior hyperlinks between properties. Based upon line-of-sight, wireless bridges are not impacted through hurdles including expressways, railroads, and bodies of water, which generally posture trouble for copper as well as the fibre-optic wire.

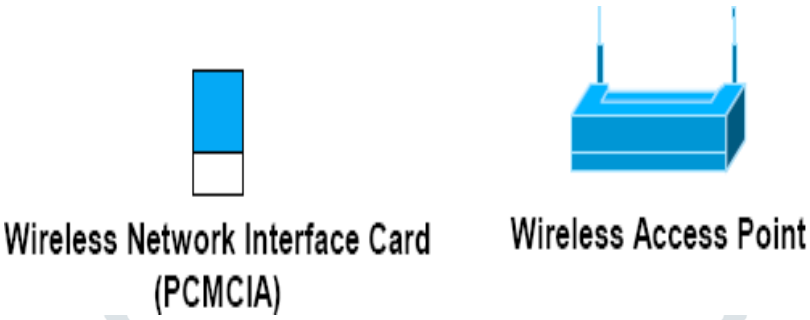

Figure 1: Basic components of WLAN

III. THREATS AND VULNERABILITIES

Figure 2 provides a primary taxonomy of security attacks to help companies and also consumers comprehend several of the attacks against WLANs.

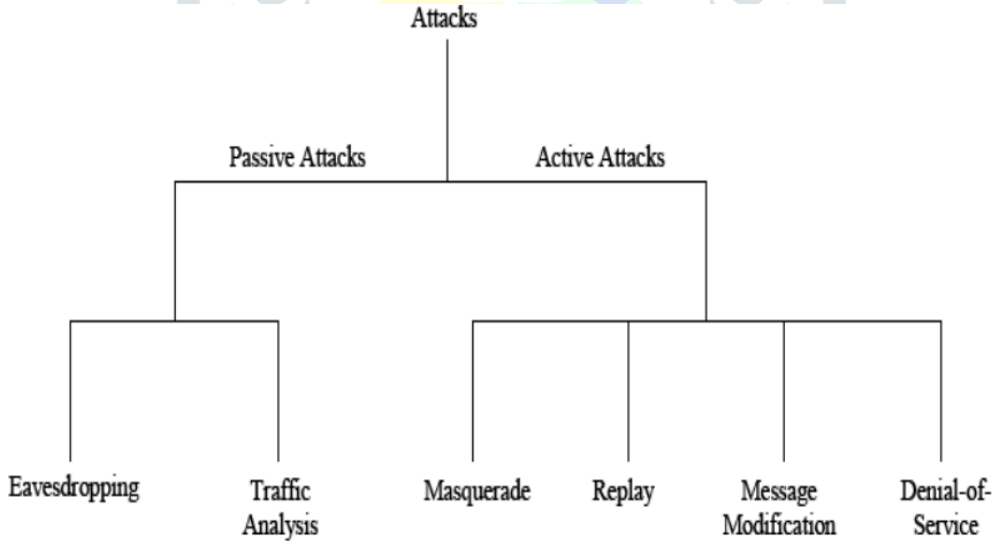

Figure 2: Taxonomy of Security Attacks

Network security attacks are generally divided into passive as well as energetic strikes. These two vast training class are actually after that subdivided right into various other types of assaults.

1) Static Spell-- An attack through which an unapproved celebration gains access to a resource as well as performs certainly not tweak its information (i.e., eavesdropping). Easy spells may be either eavesdropping or even website traffic evaluation (in some cases referred to as visitor traffic flow study). These two easy spells are defined listed below.

Eavesdropping-- The assailant observes transmissions for notification web content. An instance of this particular assault is a personal listening near right into the broadcasts on a LAN between two workstations or even tuning in to sendings between a wireless mobile as well as a base station.

Web traffic review-- The opponent, in a more subtle way, increases notice by keeping track of the broadcasts for patterns of communication. A significant volume of information it had in the circulation of notifications in between connecting celebrations.

2) Active Attack-- An attack whereby an unwarranted party creates modifications to a notification, records flow, or even documents. It is achievable to detect this kind of attack, yet it might certainly not be avoidable. Active attacks might take the type of some of four styles: Masquerading, Replay, Message modification, and Denial-Of-Service (DoS). These assaults are determined listed below.

Impersonating-- The attacker impersonates a certified customer and also there through increases specific unwarranted opportunities.

Replay-- The assailant monitors transmissions(passive assault) and retransmits information as the legit user.

Notification customization-- The aggressor alters valid information by erasing, adding to, changing, or even reordering it.

Denial-of-service-- The enemy avoids or bans the usual usage or even management of interactions resources.

The threats linked with 802.11 are the result of one or more of these strikes. The repercussions of these assaults consist of, however, are not confined to, reduction of exclusive info, legal and rehabilitation expenses, stained image, as well as the loss of network service. As the number of organizations that deploy wireless networks remains to grow, it ends up being a lot more crucial to comprehend the forms of vulnerabilities and also threats encountering tradition IEEE 802.11 WLANs and implement appropriate security solutions. Several of the vulnerabilities that are described are inherent in the legacy IEEE 802.11 WLAN criterion, while others relate to WLANs or wireless social network typically.

3) Loss of Discretion

Because of the program and also radio attribute of wireless technology, ensuring discretion is substantially more difficult in a wireless network than a wired network. Standard wired networks supply inherent security through using a bodily tool to which an aggressor requires to access. Wireless networks multiply signs into the room, creating traditional bodily security countermeasures less reliable as well as access to the system a lot easier, boosting the significance of adequate discretion on wireless networks.

Passive eavesdropping on heritage IEEE 802.11 WLAN interactions might trigger considerable risk to a company. An opponent can check Radio Frequency signals and also grab data going across the wireless tool. Vulnerable info, including exclusive information, network I.d.s and codes, and even set up records, are some instances of information that might be grabbed. On top of that, aggressors along with high-gain aerials may capture records coming from wireless networks beyond a network's typical operating variation, again creating discretion a vital security step.

Eavesdropping performed with a wireless network analyzer resource or sniffer is incredibly quick and easy for heritage IEEE 802.11 WLANs. Sniffers may make use of problems in the key-scheduling formula that was offered the execution of RC4 made use of through WEP. To make use of these weak spots, the nose passively keeps an eye on the WLAN and figures out the security secrets after a changeable amount of packets have been smelled. On a very saturated network, collecting the amount of information required to calculate the WEP tricks only takes many hrs; if website traffic volume is reduced, it might use up to one day. For instance, a busy AP that is transferring 3,000 bytes at 11 Mbps will run through the 24-bit IV room after roughly 10 hrs. As soon as the aggressor recoups 2 cypher messages that have made use of the same IV, both records honesty, as well as discretion, may be risked.

Another danger to WLANs is the reduction of discretion through straightforward eavesdropping on program web traffic. Ethernet centres typically broadcast network web traffic to all physical user interfaces and hooked up gadgets, which leaves the broadcasted visitor traffic susceptible to unauthorized monitoring. As an example, an AP attached to a port on an Ethernet centre that is broadcasting records website traffic would disclose each one of the records markets it gotten on its wired interface over its wireless interface. The use of the Ethernet hub framework enhances the risk that the AP might be relaying complete or sensitive information that was broadcast with the hub. Switches ease this worry by giving committed networks between communication devices.

A harmful or irresponsible individual can surreptitiously literally put a fake AP into a closet, under a meeting rooms table, or in every other surprise place within a structure. The rogue AP might at that point be utilized to enable unwarranted people to access to a business network. So long as its location remains near the consumers of the

WLAN, as well as it is set up to appear as a legitimate AP to wireless customers, the rogue AP may successfully entice wireless clients of its legitimacy and lead to wireless clients to link and transmit visitor traffic to the fake AP.

Within this scenario, an assaulter can effortlessly catch each one of the records sent through the rogue AP, bypassing all wireless process discretion. It is also essential to take note that not all rogue APs are released through destructive users. Often, rogue APs are set up by customers that wish to benefit from wireless technology without the confirmation of the IT division. These APs are commonly set up without effective security setups and position significant security risks.

Reduction of Honesty

Records honesty problems in wireless networks are similar to those in wired networks. Because associations regularly execute wireless and wired communications without enough cryptographic defence of records, stability may be challenging to accomplish. For instance, an aggressor may endanger records honesty through erasing or customizing the information in an email through the wireless system. This can be detrimental to an institution if the necessary email is commonly distributed amongst email recipients since the security functions of the legacy IEEE 802.11 specification does not provide inflexible message integrity, various other types of active spells that risk device honesty is feasible.

Loss of Schedule

A denial of WLAN supply usually entails some form of DoS attack, like jamming or even flooding. Sticking develops when an RF sign given off from a wireless unit overwhelms other wireless tools and indicators, causing a reduction of communications. Congesting may be triggered purposely through a destructive consumer or started inadvertently through discharges from other reputable units running within unlicensed range, such as a cord-less telephone or even microwave oven. Flooding attacks are initiated using software application made to transfer a multitude of packets to an AP or other wireless gadget, causing the device to become confused through packages and end usual operation. Flooding can trigger a WLAN to break down to an improper functionality level or maybe stop working altogether. Sticking as well as swamping threats, are difficult to counter in any radio-based communications, as well as the tradition IEEE 802.11 specification does certainly not give any defence against all of them.

IEEE 802.11 management frames give one more angle for DoS attacks against WLANs. Monitoring frameworks control the method of associating and also disaffiliating APs as well as STAs coming from a WLAN. Deliberately, the IEEE 802.11 criterion does undoubtedly not deliver security against these attacks. If an enemy forges a disassociation structure as well as provides it to an AP or even STA, the targeted gadget will undoubtedly grant the demand and also close its own communications association. Another type of attack, referred to as an affiliation attack, targets an AP's association table, which tracks the condition of STAs related to the AP. An association typically strike floodings this table with misleading asks for until the AP no longer permits legitimate organizations. Advanced association spells may push STAs to connect to devious APs where the sufferer undergoes a wide array of malicious attacks.

Users can easily additionally result in a loss of absence by unintentionally monopolizing the ability of a WLAN, such as installing big files, effectively denying various other individuals access to the network..

IV. WLAN SECURITY ATTACKS

Generally, security problems in the WLAN world are classified right into physical as well as logical. There are many security threats and attacks that can harm the security of WLANs. Those attacks could be identified right into logical attacks and also physical attacks.

Logical Attacks

MAC COMPUTER Handle Spoofing: MACINTOSH handles are delivered in the clear when communication in between STAs and also AP takes place. A method to safeguard access to APs and as a result to the network is done to refuse various other users coming from paying attention to the communication. Honesty suggests keeping the accurateness as well as the correctness of details transferred between STAs as well as AP. Any security remedy ought to attain these three targets with each other. The security, as well as administration problem, come to be large as even more APs, are installed in the network. Thus there is a demand to rationalize and deal with security concerns in little WLANs along with big ones as well as a requirement to create approaches to resist security threats. As WLANs applications like wireless Web and wireless e-commerce spreading fast, there is a requirement to ensure the security of such applications.

Attacks on WEP: Wired Matching Privacy (WEP) is a security protocol based on security algorithm known as "RC4" that aims to finance to the WLAN comparable to the security delivered in the wired LAN. WEP possesses lots of drawbacks like the utilization of small Initialization Angle (IV) and also short RC4 security secret as well as using XOR operation to cypher the key with the plain text to produce ciphertext message. Sending the MACINTOSH deals with and also the IV in the clear aside from the frequent use a single IV and the fact that hidden tricks are shared in between communications parties are WEPs major security issues.

Rejection of Service attack: Rejection of Service attacks or DoS is a severe risk on both wired and wireless networks. This attack strives to disable the availability of the system as well as the companies it supplies. In WLANs, DoS is carried out in many techniques like conflicting the regularity range by outside RF sources, therefore, rejecting accessibility to the WLAN or even, in absolute best instances, providing get access to with reduced records prices.

Man-in-the-middle attack: This is a well-known attack in both wired as well as wireless networks. An unauthorized STA obstructs the communication between genuine STAs and the AP. The prohibited STA fools the AP and professes to be a legitimate STA; on the contrary, it also blockheads the other end STA and claims to become trusted AP. The Figure 3 series Man-in-Middle attack.

Figure 3: Representation of Man-in-Middle attack

Negative network-style: WLANs work as an expansion to the wired LAN. As a result, the security of the LAN relies very on the protection of the WLAN. The weakness of WLANs means that the wired LAN is straight on risk. An effective WLAN style needs to be applied through attempting to separate the WLAN from the wired LAN by placing the WLAN in the Demilitarized Zone (DMZ) along with firewall software, changes and any extra gain access to management technology to restrict the accessibility to the WLAN. I am additionally committing particular subnets for WLAN than the once used for wired LAN might assist in curbing security violations. Cautious wired and also wireless LAN network-style plays a necessary part to protect access to the WLAN.

Default AP setups: The majority of APs are shipped with the minimum required or no security configuration through nonpayment. This holds considering that delivering them along with all security components allowed are going to make consumption as well as operation difficult for regular consumers. The purpose of AP suppliers is actually to supply higher information fee, away from the box installation APs without a sincere commitment to security. Network security managers must configure these AP according to the companies security policy. Some of the default unsecured settings in APs transported today are default passwords which occur to become weak or empty.

SSID: Service Specify Identifier (SSID) is the name provided a specific WLAN, and it is introduced due to the AP, the know-how of SSID is essential and functions as the first security self-defence. Regrettably, by nonpayment, some APs disable SSID ask for which means individuals can easily access the WLAN without confirming the expertise of SSID. Meanwhile, some APs don't undermine SSID demand; in reality, the SSID demand is made it possible for however, the SSID name itself is broadcasted in the air. This is yet another security concern given that it advertises the life of the WLAN. SSID demands should be permitted as well as SSID names shouldn't be announced; therefore, individuals have to show the expertise of WLAN's SSID before developing communication.

Physical attacks

Rogue Get Access To Points: In everyday situations, AP certifies STAs to grant access to the WLAN. The AP is never asked for authorization if the AP is mounted without the IT centre's understanding. These APs are gotten in

touch with "Rogue APs", and also they develop a security gap in the network. An aggressor can quickly put in a Rogue AP with security functions impaired resulting in a mass security hazard. There is a requirement for reciprocal verification between STAs and APs to make sure that each party are legitimate. Network security administrators may find out Fake APs by using wireless analyzing resources to search as well as investigate the network.

The physical positioning of APs: The setup location of APs is another security issue because placing APs wrongly will expose it to physical attacks. Attackers may quickly recast the APs as soon as found triggering the AP to switch over to its nonpayment settings which are unprotected. It is quite vital for network security administrators to correctly pick suitable locations to install APs.

V. CONCLUSION

The principal difference between WLANs and wired/fixed LANs is that WLANs counts on Superhigh frequency (Radio Frequency) signals as a communication tool. The signs broadcasted by the AP can easily circulate outside the perimeter of a space or even a building, where an AP is positioned, allowing individuals who are not actually in the property to get to the network. Attackers make use of special devices and smelling devices to locate accessible WLANs and tune in on online interactions while steering an auto or strolling about. Because Radio Frequency signs obey no limits, aggressors outside a building may get such signals and also launch attacks on the WLAN. This type of attack is referred to as "battle driving". Publicly accessible resources are utilized for battle driving like Net Stumbler. Enthusiasts additionally chalk structures to suggest that signs are actually broadcasted from the system, and the WLAN may be effortlessly accessed. This branding is even named "war chalking". In War liquid chalking, info regarding the velocity of the relationship and also whether the verification system used is open or shared keys are pointed out in the form of exclusive codes set in between war-chalkers. This paper provided the representation of man-in-middle attack and WLAN security attacks.

REFERENCES

[1] Prof. Satish K. Shah, Ms. Sonal J Rane, Ms. Dharmistha D Vishwakarma (2012) "Performance Evaluation of Wired and Wireless Local Area Networks" International Journal of Engineering.Research and Development

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

[3] SachiPandey, VibhoreTyagi(2013) "Performance Analysis of Wired and Wireless Network using NS2 Simulator" International Journal of Computer Applications.

[4] KarthikLakshminarayanan, Venkata N. Padmanabhan, JitendraPadhye "Bandwidth Estimation in Broadband Access Networks".

[5] Peddyreddy. Swathi, "Approaches And Objectives towards Financial Management", International Journal of Advanced in Management, Technology and Engineering Sciences, Volume IV, Issue I, 2014

[6] Peddyreddy. Swathi, "An Overview On The Types Of Capitalization", International Journal of Advanced in Management, Technology and Engineering Sciences, Volume VI, Issue I, 2016

[7] Peddyreddy. Swathi, "Architecture And Editions of Sql Server", International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Volume 2, Issue 4, May-June-2017

[8] Peddyreddy. Swathi, "Scope of Financial Management and Functions of Finance", International Journal of Advanced in Management, Technology and Engineering Sciences, Volume III, Issue 1, 2013

[9] Peddyreddy. Swathi, "A Study On Security Towards Sql Server Database", JASC: Journal of Applied Science and Computation, Volume V, Issue II, February 2018

[10] Peddyreddy. Swathi, "A Comprehensive Review on The Sources of Finance", International Journal of Scientific Research in Science, Engineering and Technology, Volume 1, Issue 4, July-August 2015

[11] Peddyreddy. Swathi, "A Study on SQL - RDBMS Concepts And Database Normalization", JASC: Journal of Applied Science and Computations, Volume VII, Issue VIII, August 2020

[12] Peddyreddy. Swathi, "A Comprehensive Review on SQL - RDBMS Databases", Journal of Emerging Technologies and Innovative Research, Volume 6, Issue 3, March 2019.

[13] Peddyreddy. Swathi, "An Overview on the techniques of Financial Statement Analysis", Journal of Emerging Technologies and Innovative Research, Volume 1, Issue 6, November 2014

[14] Peddyreddy. Swathi, "COMPLEXITY OF THE DBMS ENVIRONMENT AND REPUTATION OF THE DBMS VENDOR", Journal of Interdisciplinary Cycle Research, 13 (3), 2054-2058

[15] Peddyreddy. Swathi, "Implementation of AI-Driven Applications towards Cybersecurity", JASC: Journal of Applied Science and Computations, 7(8), 127-131

[16] Peddyreddy. Swathi. (2022). Implications For Research In Artificial Intelligence. Journal of Electronics,Computer Networking and Applied Mathematics(JECNAM) ISSN : 2799-1156, 2(02), 25–28. Retrieved from http://journal.hmjournals.com/index.php/JECNAM/article/view/447

[17] Peddyreddy. Swathi. (2022). A Study On The Restrictions Of Deep Learning. Journal of Artificial Intelligence,Machine Learning and Neural Network (JAIMLNN) ISSN: 2799-1172, 2(02), 57–61. Retrieved from http://journal.hmjournals.com/index.php/JAIMLNN/article/view/444

[18] Peddyreddy. Swathi. (2022). Industry Applications of Augmented Reality and Virtual Reality. Journal of Environmental Impact and Management Policy(JEIMP) ISSN:2799-113X, 2(02), 7–11. Retrieved from http://journal.hmjournals.com/index.php/JEIMP/article/view/453

[19] Kola Vasista. (2022). Benefits And Approaches Of Artificial Intelligence. Journal of Artificial Intelligence,Machine Learning and Neural Network (JAIMLNN) ISSN: 2799-1172, 2(02), 52–56. Retrieved from http://journal.hmjournals.com/index.php/JAIMLNN/article/view/443

[20] Kola Vasista. (2022). Practical Approach Of Implementing Artificial Intelligence. Journal of Electronics,Computer Networking and Applied Mathematics(JECNAM) ISSN : 2799-1156, 2(02), 21–24. Retrieved from http://journal.hmjournals.com/index.php/JECNAM/article/view/445

[21] Vasista, K. (2022). Evolution of AI Design Models. Central Asian Journal Of Theoretical & Applied Sciences, 3(3), 1-4. Retrieved from https://cajotas.centralasianstudies.org/index.php/CAJOTAS/article/view/415

[22] Vasista, K. (2022). Augmented Reality Vs. Virtual Reality. Central Asian Journal Of Mathematical Theory And Computer Sciences, 3(3), 1-4. Retrieved from https://cajmtcs.centralasianstudies.org/index.php/CAJMTCS/article/view/154

[23] Kola Vasista. (2022). Implications for Policy and Practice Towards VR and AR. Journal of Environmental Impact and Management Policy(JEIMP) ISSN:2799-113X, 2(01), 13–17. Retrieved from http://journal.hmjournals.com/index.php/JEIMP/article/view/452

[24] Kola Vasista, "Foreign Capital Issuance and Participants in the Securities Market", International Journal of Research and Analytical Reviews, VOLUME 2, ISSUE 4, OCT. – DEC. 2015

[25] Kola Vasista, "A Research Study On Major International Stock Market", International Journal of Research and Analytical Reviews, VOLUME 4, ISSUE 3, JULY – SEPT. 2017
[26] Kola Vasista, "A Review On The Various Options Available For Investment", International Journal Of Creative Research Thoughts - IJCRT (IJCRT.ORG), Volume 7, Issue 2, April 2019, ISSN: 2320-2882
[27] Kola Vasista, "Types And Risks Involved Towards Investing In Mutual Funds", International Journal of Current Science (IJCSPUB), Volume 12, Issue 1, March 2022 , ISSN: 2250-1770
[28] Kola Vasista, "Role Of a Stock Exchange In Buying And Selling Shares", International Journal of Current Science (IJCSPUB), Volume 12, Issue 1, March 2022 , ISSN: 2250-1770
[29] Kola Vasista, "A Detailed Study On The Factors Influencing The Price Of a Stock", International Journal of Novel Research and Development, Volume 2, Issue 8, August 2017, ISSN: 2456-4184
[30] Kola Vasista, "Objectives And Importance Of Capital Markets And The Role Of Financial Institutions", International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, Vol.2, Issue 9, page no.475-478, September-2015, Available :http://www.jetir.org/papers/JETIR1701762.pdf
[31] Kola Vasista, "An Overview On Provident Fund, Pension Funds, Pfrda, Insurance Companies And IRDA", International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, Vol.5, Issue 10, page no.284-287, October-2018, Available :http://www.jetir.org/papers/JETIR1810A93.pdf
[32] Kola Vasista, "Regulatory Compliance and Supervision of Artificial Intelligence, Machine Learning and Also Possible Effects on Financial Institutions", International Journal of Innovative Research in Computer and Communication Engineering, Volume 9, Issue 6, June 2021
[33] Kola Vasista, "Micro-Financial Analysis And A Schematic View of Ai, Machine Learning and Big Data Analytics On Financial Markets", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), Volume 7, Issue 3, 2021
[34] Kola Vasista, "Implications of AI and Machine Learning Applications Towards Financial Markets", International Journal of Scientific Research in Science and Technology (www.ijsrst.com), Volume 4, Issue 2, 2018
[35] Kola Vasista, "Scope for the Usage of AI and Machine Learning in Portfolio Management and Possible Effects on Consumers and Investors", "International Journal of Innovative Research in Science, Engineering and Technology", Volume 5, Issue 2, Feb 2016
[36] Anumandla Mounika, "Threats, Opportunities Of The Cloud And Provision Of Application Services", JASC: Journal of Applied Science and Computations, Volume 2, Issue 1, Jan-June 2015
[37] Anumandla Mounika, "Security And Privacy Issue Towards Data Security In Cloud Computing", JASC: Journal of Applied Science and Computations, Volume 1, Issue 1, January-June 2014
[38] Anumandla Mounika Reddy, "IOT data discrimination and data protection", International Journal of Academic Research and Development, Volume 6, Issue 5, 2021, Page No. 20-22
[39] Anumandla Mounika, "Data Security In The Cloud", The International journal of analytical and experimental modal analysis, Volume 1, Issue 4, July-December-2012
[40] Anumandla Mounika, "A Review On Cloud Computing Platforms And Enterprise Cloud Computing Paradigm", The International journal of analytical and experimental modal analysis, Volume III, Issue II, July-November-2011
[41] Anumandla Mounika, "An Overview On The Architectural Components Of Cloud", International Journal of Research, Volume 6, Issue 12, December 2017
[42] Anumandla Mounika, "A Study On Cloud Computing Strategy Planning And Sla Management In Cloud", International Journal of Research, Volume 7, Issue 7, JULY 2018
[43] Anumandla Mounika, "Process Of Migrating Into a Cloud And Issues In Cloud Computing", Journal of Interdisciplinary Cycle Research, Volume 2, Issue 1, January-June-2010
[44] Anumandla Mounika, "Cloud Computing Infrastructure And Cloud Adoption Challenges", Journal of Interdisciplinary Cycle Research, Volume VI, Issue II, July-December 2014
[45] Anumandla Mounika, "Technical Benefits And Architecting Cloud Applications In The Aws Cloud", Parishodh Journal, Volume VIII, Issue III, March-2019
[46] Anumandla Mounika Reddy, "Service and deployment service models, IOT physical servers and cloud offerings", International Journal of Advanced Research and Development, Volume 6, Issue 4, 2021, Page No. 5-7
[47] Anumandla Mounika Reddy, "A Review on IoT Enabled Technologies and Back-End Data-Sharing Model", "Journal of Electronics, Computer Networking and Applied Mathematics", Vol 01, No. 01, Aug-Sep 2021
[48] Anumandla Mounika Reddy, "Unique Privacy Aspects of Internet of Things", "Journal of Artificial Intelligence, Machine Learning and Neural Network", Vol 01, No. 01, Aug-Sep 2021
[49] Anumandla Mounika, "A Review on Applications of Artificial Intelligence for Public Cloud", International Journal of Scientific Research & Engineering Trends, Volume 7, Issue 3, May-June-2021
[50] Satya Nagendra Prasad Poloju, "Data Mining As a Support For Business Intelligence Applications To Big Data", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.7, Issue 2, pp.850-854, April 2019, Available at :http://www.ijcrt.org/papers/IJCRT1134576.pdf
[51] Satya Nagendra Prasad Poloju, "Big Data Analytics: Data Pre-Processing, Transformation And Curation", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.5, Issue 2, pp.835-839, May 2017, Available at :http://www.ijcrt.org/papers/IJCRT1134573.pdf
[52] Satya Nagendra Prasad Poloju, "Applications Of Big Data Technology And Cloud Computing In Smart Campus", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.1, Issue 2, pp.840-844, September 2013, Available at :http://www.ijcrt.org/papers/IJCRT1134574.pdf
[53] Satya Nagendra Prasad Poloju, "Relevant Technologies of Cloud Computing System", International Journal of Engineering Research and Applications, ISSN: 2248-9622, Vol. 4, Issue 4, (Version-3) April 2014, pp. 74-78, Available at: https://www.ijera.com/pages/v4no4(v3).html
[54] Satya Nagendra Prasad Poloju, "Service Models Towards The Evolution Of Cloud Computing", International Journal of Engineering Research and Applications, ISSN: 2248-9622, Vol. 10, Issue 6, (Series-VIII) June 2020, pp. 77-81, Available at: https://www.ijera.com/pages/v10no6.html
[55] Satya Nagendra Prasad Poloju, "Global Optimization Of Complex Systems With Big Data", International Journal of Novel Research and Development (www.ijnrd.org), ISSN:2456-4184, Vol.1, Issue 3, page no.1-6, December-2016, Available :http://www.ijnrd.org/papers/IJNRD1612001.pdf
[56] Satya Nagendra Prasad Poloju, "Techniques For Improving Network Performance Using Big Data", International Journal of Novel Research and Development (www.ijnrd.org), ISSN:2456-4184, Vol.3, Issue 3, page no.64-69, March-2018, Available :http://www.ijnrd.org/papers/IJNRD1803015.pdf
[57] Satya Nagendra Prasad Poloju, "A Survey On Big Data Driven Networking And Cloud Computng Service Models", IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P- ISSN 2349-5138, Volume.1, Issue 3, Page No pp.591-596, July 2014, Available at : http://www.ijrar.org/IJRAR19D3651.pdf
[58] Satya Nagendra Prasad Poloju, "Evolution Of Data Mining Technique To Big Data Analytics And Big Data Analytics-Powered Industrial Solutions", IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P- ISSN 2349-5138, Volume.5, Issue 4, Page No pp.584-590, November 2018, Available at : http://www.ijrar.org/IJRAR19D3650.pdf
[59] Satya Nagendra Prasad Poloju, "Big Data Analytics-Powered Design Cycle And Deployment Of Big Data Analytics In The Cloud", International Journal of Emerging Technologies and Innovative Research (www.jetir.org | UGC and issn Approved), ISSN:2349-5162, Vol.9, Issue 5, page no. ppd218-d223, May-2022, Available at : http://www.jetir.org/papers/JETIR2205446.pdf
[60] Satya Nagendra Prasad Poloju, "Cloud Computing Environments For Big Data", International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, Vol.4, Issue 9, page no.827-830, September 2017, Available :http://www.jetir.org/papers/JETIR1709122.pdf
[61] Satya Nagendra Prasad Poloju, "A Study On The Principles Associated With Cloud Computing", Strad Research, VOLUME 6, ISSUE 12, 2019
[62] Satya Nagendra Prasad Poloju, "Comparison Of Cloud Computing Deployment Models And Web 2.0 Interfaces To The Cloud", Strad Research, VOLUME 8, ISSUE 2, 2021
[63] Adithya Vuppula, "Classification and Visualization of Data Mining Model", "International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering", Vol. 4, Issue 8, August 2015

[64] Adithya Vuppula, "Data Mining: Convergence of Three Technologies", "International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering", Vol. 7, Issue 6, June 2018
[65] Adithya Vuppula, "Initiatives of 5G Vision and 5G Standardization", International Journal of Innovative Research in Computer and Communication Engineering", Vol. 6, Issue 2, February 2018
[66] Adithya Vuppula, "Security Mechanisms for IOT Services and Differences between IOT and Traditional Networks", "International Journal of Innovative Research in Science, Engineering and Technology", Vol. 6, Issue 2, February 2017
[67] Adithya Vuppula, "Communication and Protocols towards IOT Based Security", "International Journal of Innovative Research in Science, Engineering and Technology", Vol. 3, Issue 10, October 2014
[68] Adithya Vuppula, "Principles of Wireless Networking and Radio Transmission Technology", "International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering", Vol. 1, Issue 2, August 2012
[69] Adithya Vuppula, "Integrating Data Mining with Cloudusing Four Levels of Data Mining Services", "International Journal Of Multidisciplinary Research In Science, Engineering and Technology (IJMRSET)", Volume 4, Issue 5, May 2021
[70] Adithya Vuppula, "A Study on Minnesota Intrusion Detection System (Minds)", "International Journal Of Multidisciplinary Research In Science, Engineering and Technology (IJMRSET)", Volume 1, Issue 1, November 2018
[71] Adithya Vuppula, "Optimization Of Data Mining And The Role Of Big Data Analytics In Sdn And Intra-Data Center Networks", International Journal of Science & Engineering Development Research (www.ijsdr.org), ISSN:2455-2631, Vol.1, Issue 4, page no.389 - 393, April-2016, Available :http://www.ijsdr.org/papers/IJSDR1604070.pdf
[72] Adithya Vuppula, "Efficiency And Scalability Of Data Mining Algorithms", International Journal of Science & Engineering Development Research (www.ijsdr.org), ISSN:2455-2631, Vol.4, Issue 9, page no.322 - 328, September-2019, Available :http://www.ijsdr.org/papers/IJSDR1909045.pdf
[73] Adithya Vuppula, "An Overview on the Types of Wireless Networks", "International Journal of Innovative Research in Computer and Communication Engineering", Vol. 1, Issue 9, November 2013
[74] Adithya Vuppula, "Bonferroni's Principle for The Categorization Data Mining Systems", International Journal of Scientific Research in Science and Technology (www.ijsrst.com), Volume 2, Issue 5, September-October-2016
[75] Adithya Vuppula, "Applying Data Mining Techniques Towards Exploring Variables Using Weka Explorer Interface", "Shodhshauryam, International Scientific Refereed Research Journal", Volume 1, Issue 2, July-August-2018
[76] Vasundhara D.N, Seetha M, "Rough-set and artificial neural networks-based image classification", 2nd International Conference on Contemporary Computing and Informatics (IC3I) 2016, 35-39.
[77] D.N. Vasundhara, M. Seetha, "Accuracy assessment of rough set based SVM technique for spatial image classification", International Journal of Knowledge and Learning, Vol. 12, No. 3, 2018, 269-285.
[78] Dr. R. LAKSHMI TULASI, M.RAVIKANTH, "Intrusion Detection System Based On 802.11 Specific Attacks", International Journal of Computer Science & Communication Networks, Vol 1, Issue 2, Nov 2011
[79] Ravikanth, Suresh.CH, Sudhakar Yadav.N, "Image Based Kitchen Appliances Recognition And Recommendation System", GIS SCIENCE JOURNAL, Vol.8, Issue No. 12, December 2021
[80] Dr. Joel Sunny Deol Gosu, Dr. Pullagura Priyadarsini Ravi Kanth Motupalli, "A Hybrid Approach for the Analysis of Feature Selection using Information Gain and BAT Techniques on The Anomaly Detection", Turkish Journal of Computer and Mathematics Education, Vol.12, No. 5, April 2021
[81] D.N. Vasundhara, M. Seetha, "Hybrid Classification Models using ANN and Fuzzy Support Vector Machines on Spatial Databases", Data Mining and Knowledge Engineering, Vol.7, Issue 8, 2015, 279-282.
[82] D.N. Vasundhara, M. Seetha, "Implementation of hybrid RS-ANN for spatial image classification", 2016 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), 2016, 1-5.
[83] D.N. Vasundhara, M. Seetha, "Implementation of Spatial Images Using Rough Set-Based Classification Techniques", Advances in Intelligent Systems and Computing, Volume 1090, 2020, 453-466.
[84] Ravi Kanth Motupalli, Dr. O. Naga Raju, "Integration of SQL Modelling and Graph Representations to Disaggregated Human Activity Data for Effective Knowledge Extraction", Psychology And Education, Volume 57, Issue 8, 2020
[85] Kota Chaitanya Kumar, Ravi Kanth Motupalli, "Arduino Uno based Smart Helmet with Protective Bike System Using IoT", Jour of Adv Research in Dynamical & Control Systems, Vol. 12, No. 9, 2020
[86] Ravi Kanth Motupalli, Dr. O. Naga Raju, "A Systematic Review on Modelling of Human Activity Patterns in Smart Homes", "Science, Technology and Development", Volume VIII , Issue XII, Dec 2019
[87] Chalumuru Suresh, Ravi Kanth Motupalli, Srivani.B, Venkata Krishna Rao.M,Somula Ramasubbareddy, "Predicting Students' Transformation To Maximum Depressive Disorder And Level Of Suicidal Tendency", International Journal of Advanced Science and Technology, Volume 29, No. 7s, 2020
[88] Madhavi Latha Navuluri, Ravikanth Motupalli, "Enabling Smart Cities through the frame work of IOT", International Journal of Research and Analytical Reviews, Volume 6 , Issue 1, Jan 2019
[89] D.N. Vasundhara, M. Seetha, "Rough Set based SVM Technique for Spatial Image Classification", International Journal of Control Theory and Applications, Volume 9, Issue 44, 2017, 365-378.
[90] Venkata Krishna Rao, Ch Suresh, K. Kamakshaiah, M. Ravikanth, "Prototype Analysis for Business Intelligence Utilization in Data Mining Analysis", International Journals of Advanced Research in Computer Science and Software Engineering, Volume 7, Issue 7, July 2017
[91] P Ramakrishna, M Ravikanth, "Provable Data Possession & Analysis of Cloud's Data using Fuzzy Clustering", International Journal of Engineering Science & Advanced Technology, Volume-6 , Issue-1, Feb 2016
[92] Shaik. Kareem Basha, L. Harika, M. Ravi Kanth, "List Search Algorithm using Queue", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 12, Dec 2014
[93] Dr. R. LAKSHMI TULASI, M.RAVIKANTH, "Impact of Feature Reduction on the Efficiency of Wireless Intrusion Detection Systems", International Journal of Computer Trends and Technology, July-Aug 2011
[94] Anthony C. Ijeh, Allan J. Brimicombe, David S. Preston, Chris .O. Imafidon "Security Measures in Wired and Wireless Networks"