© 2018 IJSRST | Volume 4 | Issue 10 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

An Overview of Security Mechanisms Towards Different Types of Attacks

Anusha Medavaka

Software Programmer, Seven Hills IT Solutions LLC, New Jersey

ABSTRACT

Protection is a basic part in the computing and also networking innovation. The most importantly point of every network making, planning, structure, and operating a network is the significance of a solid safety and security plan. Network safety has come to be more important to desktop computer customers, organizations, and also the armed force. With the development of the internet, safety and security became a major issue. The internet framework itself permitted numerous security threats to occur. Network safety is becoming of terrific significance because of copyright that can be conveniently acquired through the internet. There is various type of attack that can be when sent out across the network by understanding the attack approaches, enables the appropriate safety to emerge. Several organizations secure themselves from the internet using firewalls and encryption devices. There is a large amount of individual, industrial, army, and government information on networking frameworks worldwide and all of these needed different safety systems. In this paper, we are attempting to study most different sort of attacks along with numerous different sort of protection device that can be applied according to the need and architecture of the network.

Keywords : Attacks, Network Security, Cloud-Environment Security.

I. INTRODUCTION

Network Security management is different for all sort of scenarios and also is necessary as the expanding use internet. A home or tiny workplace may only need standard security while big services might need high-maintenance as well as advanced software program as well as hardware to avoid harmful attacks from hacking as well as spamming [1] New Threats Demand New Approaches as the network is the door to your company for both legitimate users as well as prospective attackers. For several years, IT specialists have built obstacles to avoid any type of unauthorized entrance that could jeopardize the company's network. As well as this network security is very important for every network designing, planning, building, and operating that contain strong security plans. The Network Protection is continuously developing, as a result of web traffic growth, use patterns and the ever transforming risk landscape [3] For instance, the extensive fostering of cloud computer, social networking and also bring-your-own-device (BYOD) programs are presenting brand-new obstacles and threats to a currently intricate network.

According to the UK Federal government, Info safety and security is: "the technique of making certain info is just check out, listened to, altered, program and otherwise used by people that can do so" (Resource: UK Online for Service). Info systems need to be safe if they are to be trusted. Given that lots of companies are critically reliant on their details systems for key organization processes (e.g. internet sites, production organizing, purchase handling), safety can be attended

be an extremely important area for management to solve. The large topic of network protection is assessed by investigating the following:

- ✓ Background of safety in networks
- ✓ Internet architecture and also vulnerable safety elements of the Internet
- ✓ Types of internet attacks and also safety and security methods
- ✓ Safety and security for connect with internet accessibility
- ✓ Current growth in network protection software and hardware

When taking into consideration network security, it must be emphasized generally that the entire network must be remaining protected. Network protection does not only worry the protection in the computer systems at each end of the communication chain. When sending information the interaction channel should not be susceptible to attack, where the opportunities of threats are a lot more permeating. A feasible hacker can target the communication network, get the information, decrypt it as well as re insert a false message. Hence, protecting the network is just as vital as safeguarding the computer systems as well as encrypting the message which we want to be kept private.

When establishing a safe network, the following need to be considered [1]:

1. Accessibility-- authorized users are supplied the ways to connect to and also from a certain network
2. Confidentiality-- Details in the network continues to be exclusive; discloser must not be conveniently feasible.
3. Authentication-- Guarantee the users of the network are, the individual should be the individual who they say they are.
4. Integrity-- Guarantee the message has not been changed en route, the material has to be like they are sent.
5. Non repudiation-- Ensure the individual does not refute that he used the network.

As an example, Number 1 [2] shows a regular security implementation designed to protect and attach multiple components of a company network. This is the most usual style as according to the area of the network.

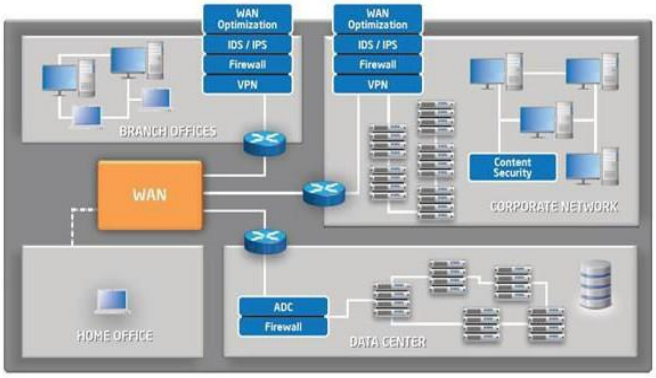

Figure1. Security present in the different kinds of the Network.

An efficient network security strategy is created with the understanding of safety and security issues, possible attackers, needed level of safety, and factors that make a network prone to attack [1] the steps involved in understanding the composition of a safe network, internet or otherwise, is complied with throughout this research study venture. Normal security presently feeds on the computers attached to the network. Protection methods often normally appear as part of a single layer of the OSI network reference version. Current work is being carried out in using a split method to secure network layout. We have actually offered the Pattern micro safety and security approach which is based upon many then solitary layers of safety and security. This safety and security method leads to an effective and effective design which circumvents several of the usual safety and security problems.

Computer innovation is a growing number of common and also the penetration of computer system in society

is a welcome step in the direction of innovation but culture needs to be far better geared up to grapple with difficulties associated with modern technology. New hacking strategies are made use of to pass through in the network and the safety vulnerabilities which are not often found create trouble for the security professionals in order to catch cyberpunks. The problems of keeping up to day with protection concerns within the realm of IT education and learning result from the absence of present info. The recent study is concentrated on bringing top quality security training incorporated with swiftly changing innovation [4] On the internet networking safety and security is to supply a solid understanding of the main problems associated with safety and security in contemporary networked computer system systems [5] This covers underlying ideas and foundations of computer system protection, standard understanding regarding security-relevant choices in developing IT facilities, methods to protect complex systems and useful abilities in taking care of a variety of systems, from personal laptop to large infrastructures. In this paper, we are briefly specifying the principle of Network Safety and security, just how it can be performed in the past. And also with the introduction as well as boosting use internet how safety threats are penetrating to our devices is additionally studied. We have discussed most of all kinds of attack that are mostly taken place on the any network including residence, office and also organizations. In the last area, we are examining various safety systems that are important to keep our network safe and secure. In this section we are covering most of the modern-day principle that appropriate for providing security, required for today's hacking as well as feasible attacks.

II. TYPES OFATTACKS

Networks go through attacks from destructive resources. As well as with the introduction and also increasing use internet connects is most typically growing on enhancing? The primary classifications of Attacks can be from 2 groups: "Easy" when a network burglar obstructs information traveling through the network, as well as "Active" in which a trespasser launches commands to interrupt the network's regular procedure [6] a system must be able to restrict damage as well as recover swiftly when attacks occur. There are some more sorts of attack that are likewise important to be thought about:

A. Passive attack

An easy attack displays unencrypted website traffic and also seeks clear-text passwords as well as delicate details that can be used in various other kinds of attacks. The monitoring and listening of the interaction network by unapproved attackers are called passive attack. It includes traffic evaluation, surveillance of unsafe communications, decrypting weakly encrypted web traffic, as well as capturing authentication details such as passwords. Passive interception of network operations enables adversaries to see forthcoming actions. Passive attacks because the disclosure of information or data files to an enemy without the authorization or understanding of the customer.

B. Active Attack

In an energetic attack, the aggressor tries to bypass or break into secured systems in the taking place communication. This can be done via stealth, viruses, worms, or Trojan steeds. Active attacks consist of attempts to prevent or break defense attributes, to present malicious code, as well as to swipe or modify details. The unauthorized attackers monitors, listens to and also customizes the data stream in the interaction network are called energetic attack. These attacks are placed versus a network backbone, make use of information in transit, digitally pass through an enclave, or attack an accredited remote customer throughout an attempt to connect to a territory. Active

attacks cause the disclosure or dissemination of data files, DoS, or modification of data.

C. Distributed attack

A dispersed attack calls for that the adversary introduce code, such as a Trojan horse or back-door program, to a-- relied on ‖ component or software application that will later be dispersed to lots of various other business as well as individuals Circulation attacks focus on the destructive adjustment of equipment or software program at the factory or during circulation. These attacks present harmful code such as a back entrance to an item to obtain unauthorized accessibility to details or to a system function at a later date.

D. Insider attack

According to a Cyber Safety and security Watch study insiders were found to be the reason in 21 percent of protection violations, and also a further 21 percent may have been due to the actions of insiders. More than half of participants to another current survey stated it's harder today to find and also avoid insider attacks than it remained in 2011, and also 53 percent were boosting their security budgets in action to expert threats [7] While a substantial number of breaches are caused by destructive or unhappy staff members - or previous employees - many are brought on by well-implying staff members that are merely trying to do their task. BYOD programs and also file sharing as well as collaboration solutions like Dropbox mean that it will certainly be tougher than ever to keep company information under business control when faced with these well-meaning but untrustworthy employees.

E. Close-in Attack

A close-in attack entails someone attempting to obtain literally near to network elements, data, and also systems in order to find out more about a network. Close-in attacks consist of regular individuals achieving close physical distance to networks, systems, or centers for the objective of modifying, celebration, or refuting accessibility to information. One prominent type of enclose attack is social engineering. In a social engineering attack, the opponent compromises the network or system through social communication with a person, via an e-mail message or phone. Numerous techniques can be made use of by the individual to revealing information concerning the protection of company. The details that the sufferer exposes to the cyberpunk would probably be utilized in a succeeding attack to gain unauthorized access to a system or network.

F. Spyware attack

A serious computer system security danger, spyware is any kind of program that checks your online activities or installs programs without your permission commercial or to record individual info. As well as this capture details is maliciously made use of as the legitimate user for that specific sort of work.

G. Phishing attack

In phishing attack the cyberpunk develops a phony internet site that looks specifically like a prominent website such as the SBI bank or PayPal. The phishing component of the attack is that the cyberpunk after that sends out an e-mail message trying to deceive the individual into clicking a web link that leads to the phony site. When the user attempts to log on with their account information, the cyberpunk videotapes the username and also password and then tries those details on the real site.

H. Hijack attack

In a hijack attack, a hacker takes over a session between you and also an additional private and separates the other individual from the interaction. You still think that you are talking with the original event as well as may send out exclusive info to the hacker by accidently.

I. Spoof attack

In the spoof attack, the hacker modifies the resource address of the packets he or she is sending to make sure that they seem originating from somebody else. This might be an effort to bypass your firewall software rules.

J. Password attack

An opponent tries to split the passwords stored in a network account database or a password-protected data. There are 3 significant kinds of password attacks: a thesaurus attack, a brute-force attack, and a crossbreed attack. A dictionary attack uses a word list data, which is a listing of possible passwords [9] a brute-force attack is when the attacker attempts every possible mix of characters.

K. Buffer overflow

A barrier overflow attack is when the opponent sends out much more information to an application than is expected. A buffer overflow attack usually results in the opponent getting management accessibility to the system in a command timely or covering.

L. Exploit attack

In this kind of attack, the enemy recognizes of a protection problem within an operating system or an item of software as well as leverages that expertise by exploiting the vulnerability.

III. TECHNOLOGIES FOR PROVIDING SECURITY TO THE NETWORK

Internet threats will certainly continue to be a significant issue in the worldwide world as long as info comes and transferred throughout the Internet. Various defense and also discovery devices were created to deal with attacks mentioned previously. A few of this mechanism along with advancement concepts are mention in this section.

A. Cryptographic systems

Cryptography is a beneficial and extensively utilized tool in protection engineering today. It included the use of codes as well as ciphers to transform information into unintelligible information.

B. Firewall

The firewall is a normal border control mechanism or perimeter defense. The purpose of a firewall program is to block website traffic from the outdoors, but it could also be used to obstruct traffic from the within. A firewall is the front line defense reaction against trespassers to go into in the system. It is a system designed to prevent unapproved access to or from a private network. Firewalls can be applied in both hardware and software, or a mix of both [9] the most commonly marketed remedy to the issues of Internet protection is the firewall program. This is a machine that stands between a neighborhood network as well as the Internet, as well as filters out website traffic that may be dangerous. The idea of a-- solution in a box ‖ has terrific interest several companies, and is now so widely approved that it's viewed as a vital part of corporate due diligence. Firewalls are available in generally 3 flavors, relying on whether they filter at the IP package degree, at the TCP session level, or at the application degree.

C. Driving Security to the Equipment Level

To even more maximize performance and also boost safety and security, Intel create systems also consist of a number of corresponding security modern technologies constructed into multiple system elements, consisting of the cpu, chipset, as well as network user interface controllers (NICs). These innovations supply reduced- degree foundation whereupon a safe as well as high carrying out network

facilities can be maintained. These technologies include Virtualization Technology, Trusted Implementation Technology and Quick Assist Innovation.

D. Intrusion Detection Equipments

An Intrusion Detection System (IDS) is an extra protection step that helps ward off computer system intrusions. IDS systems can be software application and equipment devices utilized to spot a strike. IDS items are utilized to monitor link in determining whether attacks are been released. Some IDS systems simply check and alert of an attack, whereas others try to obstruct the assault. The common antivirus software is an example of an intrusion detection system. The systems made use of to discover negative things taking place are described generically as breach detection systems. Breach discovery in company and federal government networks is a fast-growing area of safety and security research; this development has actually been triggered by the awareness that many systems make no effective use of log and also audit information.

E. Secure Outlet Layer (SSL).

The Secure Outlet Layer (SSL) is a suite of methods that is a typical means to attain a good level of protection between an internet browser as well as an internet site. SSL is designed to create a protected network, or tunnel, between an internet browser as well as the internet server, to ensure that any kind of details traded is secured within the secured passage. SSL supplies authentication of clients to web server through making use of certifications. Clients present a certificate to the server to prove their identity.

F. Dynamic Endpoint Modeling

Observable's safety and security remedy, represents an exceptionally brand-new means to take a look at IT protection. It versions each device on your network, so you can understand regular behavior and also rapidly do something about it when a device starts acting unusually. There's no need to install agents on the devices, or attempt to utilize deep-packet inspection, givingyoua powerful remedy to conquer these new safety challenges.

G. Mobile Biometrics.

Biometrics on smart phones will play a bigger duty in confirming individuals to network services, one safety exec anticipated. Biometrics emerging on mobile endpoints, either as applications that collect users' habits or as devoted features on mobile endpoints that check personal attributes. For example, the iPhone 5s finger scan, arised in 2014, these attributes are open and extensible; it can result in genuine technology in making sure the identities of remote individuals.

IV. SOME ADVANCE NETWORK SECURITY POLICIES

A. Making Safety in Clouds Atmosphere

Experts project that IT spending will enhance slightly from 2013. This increase in financial investment is mainly attributed to cloud computer [10] over half of IT companies intend to raise their investing on cloud computer to improve adaptable and reliable use of their IT resources. Intel Trusted Implementation Modern Technology (Intel TXT) is particularly designed to solidify platforms versus hypervisor, firmware, BIOGRAPHY, and also system degree attacks in digital as well as cloud environments. It does so by giving a mechanism that enforces integrity look at these pieces of software program at launch time. This makes sure the software application has actually not been changed from its known state. This TXT likewise gives the system level depend on information that higher level security applications require to enforce role-based security plans. Intel TXT enforces

control through measurement, memory securing as well as securing secrets.

B. Zero-Trust Segmentation Fostering

This design was originally developed by John Kindervag of Forrester Research and popularized as a needed evolution of traditional overlay safety and security versions. One alternative that is a strong candidate to boost the safety situation is the absolutely no-trust model. This aggressive technique to network protection keeps an eye on every item of information feasible, under the presumption that every file is a potential danger [11] it calls for that all resources be accessed in a safe manner, that accessibility control be on a need-to-know basis and purely enforced. The systems validate and also never ever count on; that all traffic be checked, logged, and evaluated and that systems be created from the within out instead of the outdoors in. It simplifies just how info safety and security is conceptualized by thinking there are no longer-- relied on ‖ interfaces, applications, website traffic, networks or users. It takes the old design-- trust however validate and inverts it, because recent breaches have proved that when an company trust funds, it does not verify.

C. Trend Micro Danger Management Provider

Due to the fact that conventional safety and security remedies no longer sufficiently secure against the developing set of multilayered threats, individuals require a brand-new strategy. Trend Micro delivers that technique with the Fad Micro Smart Security Network [12] The Smart Protection Network facilities provides innovative, real-time protection from the cloud, blocking threats prior to them reach a customer's PC or a firm's network. Leveraged across Pattern Micro's services as well as services, the Smart Defense Network incorporates distinct Internet-based, or-- in- the-cloud, ‖ innovations with lighter-weight clients. By inspecting Links, emails, and data versus constantly updated and also associated threat databases in the cloud, clients constantly have immediate access to the current defense any place they link-- from residence, within the firm network, or on the go. Trend Micro's Risk Management Services offers an extensive sight of the activities taking place in the network. The service evaluation offers a distinct network security evaluation that offers companies with substantial information on the worth of adding an over watch protection layer for an existing defense-in-depth approach [13] The over watch security layer can reveal when a breach has occurred and also, a lot more significantly, promptly do something about it to intercept it as well as remediate it to make certain that it does not occur once more. Risk Management Provider supplies a strategy to network protection that evaluates danger and gives insight on prospective voids within the current security atmosphere. The Smart Defense Network is made up of a worldwide network of risk intelligence innovations and sensors that supply comprehensive defense against all kinds of threats-- destructive documents, spam, phishing, web threats, denial of service attacks, internet vulnerabilities, and also data loss. By incorporating in-the- cloud reputation and also patent-pending connection innovations, the Smart Security Network decreases reliance on standard pattern documents downloads as well as removes the delays frequently related to desktop updates. Organizations benefit from enhanced network data transfer, minimized handling power, and also associated price savings.

D. Advanced Risk Security with Big Information

Big Data makes large feeling for security as it includes using specialized modern technologies and also techniques to accumulate, work with, store, as well as examine really enormous amounts of associated and also maybe also disparate data to reveal insights as well as patterns that would certainly or else stay obscured. Leveraging Big Data for details safety functions not only makes good sense however is required [14] Big

Data analytics can be leveraged to boost information safety and security as well as situational understanding. For instance, Big Information analytics can be utilized to examine monetary purchases, log documents, as well as network web traffic to identify abnormalities and also suspicious tasks, and to associate numerous resources of information right into a meaningful view. Data- driven information protection go back to bank fraudulence detection and anomaly-based invasion detection systems. Fraud detection is just one of one of the most visible uses for Big Information analytics. Credit card companies have actually conducted fraud discovery for decades. Nonetheless, the custom-built facilities to extract Big Data for fraud detection were not cost-effective to adapt for other fraudulence detection makes use of. Off-the-shelf Big Data devices and also strategies are currently accentuating analytics for fraudulence discovery in health care, insurance policy, and also various other fields.

V. CONCLUSION

Security is an extremely tough as well as crucial topic. Every person has a various suggestion regarding safety' policies, as well as what degrees of threat serve. The secret for constructing a safe network is to define what safety implies to your requirement of the time as well as usage. Once that has actually been specified, everything that happens with the network can be examined with respect to that policy. It is necessary to construct systems and networks as if the customer is not constantly reminded of the security system around him but Users who discover security policies and also systems also limiting will certainly find means around them. There are various sorts of attacks on the safety plans and additionally expanding with the advancement and the growing use of internet. In this paper we are attempting to study these various kinds of attacks that permeate our system. As the threats are increasing, so for protected use of our systems and also internet there are numerous different safety and security policies are also developing. In this paper we have mention some of the safety and security policies that can be utilized mainly by number of individuals and some brand-new development high qualities that fits to the today's extra permeating environments like Pattern micro security system, use of large data top qualities in providing protection, etc. Safety is everybody's company, and only with everybody's cooperation, a smart plan, and also consistent methods, will certainly it be possible.

VI. REFERENCES

[1]. A White Paper, Securing the Intelligent Network, powered by Intelcorporation. Network Security Online available: http://en.wikipedia.org/wiki/Network_security.

[2]. Network Security: History, Importance, and Future, University of Florida Department of Electrical and Computer Engineering, Bhavya Daya.

[3]. Ateeq Ahmad, —Type of Security Threats and its Prevention", Ateeq Ahmad, Int.J.Computer Technology & Applications, Vol 3 (2),750-752.

[4]. Wright, Joe; Jim Harmening (2009) "15" Computer and Information Security Handbook Morgan Kaufmann Publications Elsevier Inc p.257

[5]. Dr. G. Padmavathi, Mrs. D. Shanmugapriya, —A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks, (IJCSIS) International Journal of Computer Science and Information Security,Vol. 4, No. 1 & 2, 2009.

[6]. Network Security Types of attacks Online available: http://computernetworkingnotes.com/networ k-security-access-lists-standards-and- extended/types-of-attack.html.

[7]. Adeyinka, O., "Internet Attack Methods and Internet Security Technology," Modeling & Simulation, 2008. AICMS 08. Second Asia International Conference on, vol., no., pp.77-82, 13-15 May2008.

[8]. Ajmera Rajesh, Siripuri Kiran, " Anomaly Detection Using Data Mining Techniques in Social Networking" in "International Journal for Research

in Applied Science and Engineering Technology", Volume-6, Issue-II, February 2018, 1268-1272 ISSN : 2321-9653 , www.ijraset.com

[9]. Sugandhi Maheshwaram , "An Overview of Open Research Issues in Big Data Analytics" in "Journal of Advances in Science and Technology", Vol. 14, Issue No. 2, September-2017 ISSN : 2230-9659

[10]. Suresh Kumar Mandala, Neelima Gurrapu, Mahipal Reddy Pulyala, " A Study on the Development of Machine Learing in Health Analysis", Indian Journal of Public Health Research & Development, volume 9, Number 12, December 2018, ISSN-0976-0245(Print)-ISSN-0976-5506 (Electronic)

[11]. Suresh Kumar Mandala,Mahipal Reddy Pulyala and Sanjay Pachouri, "Being a Smart Sapien with Information Centric Networking and Cloud Computing", International Journal of Pure and Applied Mathematics,Volume 117, No. 21, 2017, 243-255,ISSN: 1311-8080 (printed version)

[12]. Suresh Kumar Mandala, Sanjay Pachouri, "performance evaluation of multi stage attacks prediction", Journal of Advanced Research in Dynamical and Control Systems, Vol. 9, September 2017, JARDCS Special Issue On Engineering Technology.

[13]. Thota Mounika, Mandala Suresh kumar, "Document Proximity: Keyword Query Suggestion Based On User Location", International Journal of Research, Volume 04, Issue 14, November 2017, e-ISSN: 2348-6848 ,p-ISSN: 2348-795X .

[14]. Syeda Sobia Farees , M. Suresh Kumar, "A Novel Approach for Protecting Location Information in Geosocial Applications ", IJIEMR, Vol 1, Issue 2, November 2016 ISSN:2456-5083

[15]. Suresh Kumar Mandala,Sanjay Pachouri, "A Reviewed Study on Financial Cyber Crime and Frauds", International Journal of Advances in Arts, Sciences and Engineering(ijoaase.com), Volume 4 Issue 9, Sep 2016, ISSN. 2320-6144 (Online)

[16]. Siripuri Kiran, Ajmera Rajesh, "A Study on Mining Top Utility Itemsets In A Single Phase" in "International Journal for Science and Advance Research in Technology (IJSART)", Volume-4, Issue-2, February-2018, 637-642, ISSN(ONLINE): 2395-1052

[17]. Yeshwanth Rao Bhandayker, "Security Mechanisms for Providing Security to the Network" in "International Journal of Information Technology and Management", Vol. 12, Issue No. 1, February-2017, ISSN : 2249-4510

[18]. Sugandhi Maheshwaram, S. Shoban Babu , "An Overview towards the Techniques of Data Mining" in "RESEARCH REVIEW International Journal of Multidisciplinary", Volume-04, Issue-02, February-2019 ISSN : 2455-3085

[19]. Yeshwanth Rao Bhandayker , "A Study on the Research Challenges and Trends of Cloud Computing" in "RESEARCH REVIEW International Journal of Multidisciplinary ", Volume-04, Issue-02, February-2019 ISSN : 2455-3085

[20]. Sriramoju Ajay Babu, Dr. S. Shoban Babu, "Improving Quality of Content Based Image Retrieval with Graph Based Ranking" in "International Journal of Research and Applications", Volume 1, Issue 1, Jan-Mar 2014 ISSN : 2349-0020

[21]. Dr. Shoban Babu Sriramoju, Ramesh Gadde, "A Ranking Model Framework for Multiple Vertical Search Domains" in "International Journal of Research and Applications" Vol 1, Issue 1,Jan-Mar 2014 ISSN : 2349-0020 .

[22]. Mounika Reddy, Avula Deepak, Ekkati Kalyani Dharavath, Kranthi Gande, Shoban Sriramoju, "Risk-Aware Response Answer for Mitigating Painter Routing Attacks" in "International Journal of Information Technology and Management", Volume VI, Issue I, Feb 2014 ISSN : 2249-4510

[23]. Sugandhi Maheshwaram, "A Review on Deep Convolutional Neural Network and its Applications" in "International Journal of Advanced Research in Computer and Communication Engineering", Vol. 8, Issue No. 2, February-2019 ISSN : 2278-1021 , DOI 10.17148/IJARCCE.2019.8230

[24]. Yeshwanth Rao Bhandayker. "An Overview : Security Solutions for Cloud Environment."

International Journal for Scientific Research and Development 7.2 (2019): 1596-1598.

[25]. Yeshwanth Rao Bhandayker. "AN OVERIEW OF CYBER SECURITY", International Journal of Research, vol. 8, Issue. 3 (2019): 2236-6124.

[26]. Sugandhi Maheshwaram, "A STUDY ON THE CHALLENGES IN HANDLING BIG DATA", International Journal of Research, vol. 8, Issue. 3 (2019): 2236-6124.

[27]. Yeshwanth Rao Bhandayker. "An Overview of Service Models and Cloud Computing Evolution in IT", International Journal of Research and Applications, vol. 5, Issue. 20, Oct - Dec 2018 Transactions 5(20) : 1000-1004. ISSN : 2349 – 0020

[28]. Yeshwanth Rao Bhandayker. "A Comprehensive Survey on Security Issues and Advantages towards Cloud Computing", International Journal of Research and Applications, vol. 5, Issue. 18,Apr - Jun 2018 Transactions 5(18): 801-807. ISSN : 2349 – 0020

[29]. Sugandhi Maheshwaram, . "A Study on Security Information and Event Management (SIEM)", International Journal of Research and Applications, vol. 5, Issue. 17, Jan - Mar 2018 Transactions 5(17): 705-708. ISSN : 2349 – 0020

[30]. Sugandhi Maheshwaram, . "A Novel Technique for Preventing the SQL Injection Vulnerabilities", International Journal of Research and Applications, vol. 5, Issue. 19, July - Sep 2018 Transactions 5(19): 901-909. ISSN : 2349 – 0020

[31]. Shoban Babu Sriramoju, "Substantial Overall Performance Pattern-matching Algorithm for Network Stability", International Journal of Research and Applications, vol. 5, Issue. 17, Jan - Mar 2018 Transactions 5(17): 701-704. ISSN : 2349 – 0020

[32]. Sugandhi Maheshwaram. "A Study Design of Big Data by Concentrating on the Atmospheric Information Evaluation." International Journal for Scientific Research and Development 7.3 (2019): 233-236.

[33]. Suresh Kumar Mandala,Sanjay Pachouri, "Analytical Study for Intrusion Detection System to Detect Cyber Attack", Airo International Research Journal, Volume VII, March 2016 ISSN: 2320-3714

[34]. Ranjeeth kumar.M, M.Suresh Kumar, S.S.V.N Sarma, "FUZZY KEYWORD SEARCH IN XML DATA", International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June 2013 ISSN : 2229-5518

[35]. Yeshwanth Rao Bhandayker, "AN OVERVIEW OF THEINTEGRATION OF ALL DATA MINING AT CLOUD-COMPUTING" in "Airo International Research Journal", Volume XVI, June 2018 ISSN : 2320-3714

[36]. Siripuri Kiran, 'Decision Tree Analysis Tool with the Design Approach of Probability Density Function towards Uncertain Data Classification', International Journal of Scientific Research in Science and Technology(IJSRST), Print ISSN : 2395-6011, Online ISSN : 2395-602X,Volume 4 Issue 2, pp.829-831, January-February 2018. URL : http://ijsrst.com/IJSRST1841198

[37]. Yeshwanth Rao Bhandayker , "Artificial Intelligence and Big Data for Computer Cyber Security Systems" in "Journal of Advances in Science and Technology", Vol. 12, Issue No. 24, November-2016 ISSN : 2230-9659

[38]. Sugandhi Maheshwaram, "A Comprehensive Review on the Implementation of Big Data Solutions" in "International Journal of Information Technology and Management", Vol. XI, Issue No. XVII, November-2016 ISSN : 2249-4510