IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 10, Issue 5, Ver. I (Sep - Oct .2015), PP 71-80
www.iosrjournals.org

Contemporary Isometric on Computer Network Security and Privacy

Dr.P.S.Jagadeesh Kumar,
Department of Computer Science and Engineering,
Don Bosco Institute of Technology, Bangalore, Karnataka – 560074.

Abstract: *This paper springs far-reaching stratagems for contemporary isometric on computer network's security and privacy. Shielding and fortifying a computer in any network and a network in any Internet is bamboozled and obligatory. Utmost trustworthy and intimate statistics are pulled amid the users through the Internet; guarding this endorsed and subjective gen is imperative. Nonetheless, plentiful exploration has been carried out in computer network security and privacy; the hackers, both morally and deceitfully control the communal and secluded data. Up-to-the-minute network security dogmas and concealment courtesy is fighting fit deliberated in this paper to benefit the network administrator and emissaries in locking stable information.*
Keywords: *Contemporary Isometric, Computer Networks, Security, Privacy*

I. Introduction

An adequate amount of research exertions has been through cryptography; secure data accretion and intrusion recognition in Computer Network and Security. The present-day cryptography contrivances, such as authentication, identification possibly will perceive and preserve alongside node conciliation round about. However, most concession deeds cannot be perceived proximate. Conniving secure routing that can shield alongside concealed node concession is an encouraging research area. At present, farthest scheme's simply cognate security metrics and barely any of them appraised another metrics. Subsequently, metrics like; QoS (quality of service) essential to be deliberated in tallying of security. Further ostentatious studies are compulsory in the forthcoming eons about other security disputes counting security energy valuation, data assertion, survivability, trust, end-to-end security, security & privacy sustenance for data centric sensor networks (DCS) and node concession dissemination. It is imperative to get educated in these extents owing to a sensor network's distinct characteristics, such as battery constriction, high catastrophe possibility nodes, at ease conceded nodes, impulsive transmission media, etc., Up until now, there has been only a little slant presented. Consequently, more readings are obligatory in these capacities. Though there are some prevailing designs for WSN that moderately elucidate these glitches, it is still conceivable to spotlight the deserted facets that can be deliberated decisive for making an acceptable reliance fashion.

II. Literature Survey

Mahfuzulhoq Chowdhury, Md Fazlul Kader et al [1] called the four key facets of WSN security: obstacles, attacks, requirements and defences. They potted the emblematic attacks along fathomed the writings on numerous imperative security concerns pertinent to the sensor networks. Their intention was to afford a wide-ranging gestalt of the prevailing WSNs security methods. Countless security disputes in WSNs persist exposed and imagine seeing further research happenings on this exhilarating topic in the yet to come eons. Sattarova Feruza Y. and Prof.Tao-hoon Kim et al [2] clinched that the fortification of network is imperative to avert loss of server resources besides to guard the network from being used for illicit devotions. The safeguard of calculating clout is pertinent only to classy equipment such as immense supercomputers. They crammed the rudiments' apropos IT security. It further brushed up the modern expertise connected to IT security. Robert Koch, Bjorn Stelte et al [3] premised that even if firewalls and ultramodern IDSs are in domicile with today's company networks, the quantity of instance's relics on a high level, and first-hand happenings are conveyed daily. Quite a few features have been recognized, which are accountable for the debauched recital of present security systems: gradually, attacks are besieged and precisely intended, and social engineering is cast off to fetch the victim to perform the malevolent manoeuvre. Using, for instance, memory sticks, tenable and remote systems and networks can, likewise, be attacked. Application layer attacks, an amassed amount of Zero-Days and the insider menace are further affinities. The precise features of these drifts cannot be replicated by present nomenclature, hence, fettering the expansion of new security schemes and strategies. The hominid remnants the feeblest connexion to the chain, aiding erudite attacks where the licit consumer is wrought with perform the camouflaged attack by himself with his official access and devoid of recognizing the head-to-head attack. To overawe these deficiencies, brand new notions for the provision and conception of users into the security procedures are essential. Di Ma and Gene Tsudik et al [4] inspected security and privacy disputes in some fresh

and evolving wireless networks. In comprehending pertinent literature, they exasperated to recognize new security and privacy contests along with shortfalls of present methods. Certain contests ascend from the enjoined, spasmodically associated and feasibly mobile, network action. Accordingly, want to antedate threats ascending from malevolent misuse of such network topographies and design suitable security kiosk-methods. Subsequently, certain developing wireless networks remain ad hoc in nature, substructure sovereign security and privacy systems are predominantly apposite. Lastly, developing wireless devices such as RSensors inspire the evolution of first-hand cryptographic nascent and decorum.

Wenye Wang, Zhuo Lu et al [5] perceived that countless security approaches and systems could be appropriate to the Smart Grid, specifically in areas that intermingle with clients. Though in the Generation/Transmission/Distribution realms, which are answerable for the procedure of power delivery, attack detection, mitigation, authentication and key management, yet persist as perplexing security disputes due to the huge network scale and more arduous necessities for security strategy. For congestion extenuation in wireless Smart Grid claims, prevailing, and methods can be willingly amended to the Markets/ Customer/Service Provider dominions, but are not appropriate or may meet complications in the Generation/Transmission/ Distribution domains because of the strict timing necessities of message carriage in this purview. The Generation/ Transmission/Distribution needs security resolution to not only guard information interchange but also sees the necessities for data communication and handling thereby airs a concrete trial for security architects. Cyber security is still under expansion in the Smart Grid, principally since information security must be reserved into account with electrical power systems. Types of the Smart Grid communication network, for example, heterogeneous devices and network structural design, delay restraints on dissimilar time scales, scalability, and differentiated competencies of entrenched expedients, make it irrefutable unfeasible to consistently organize strong security methods all over the Smart Grid. Accordingly, the Smart Grid entails well- defined security resolutions intended precisely for discrete network solicitations, making cyber security for the Smart Grid a very productive and perplexing research expanse in the imminent. Gurveen K.Sandhu, Gurpreet Singh Mann et al [6] recommended that in high-density municipal extent, there may be manifold networks like MPLS, Metro Ethernet, fibre networks, ADSL. There may also be several contending purveyors. WiMAX is a technology for a bountiful high-speed entrée to pastoral areas. It can deliver DSL resembling speeds. Further negotiations involve creating a business plan, territory maps to the region, learning the exposure region (number of base / relay stations), tower rent payment, inhabitant of the region, bandwidth necessities, agility, etc. Obtaining spectrum is also a concern. Several territory types such as hills with a slightly high density of trees, reasonable tree density, and level area with a low tree density can edict the use of WiMAX. Radio Waves are impulsive and may go further than the exposure area of the locations. Some portions of the exposure area may not get the radio waves.

Cholatip Yawut and Phattarapong et al [7] recycled Delphi practice to prophesy the future of establishment's computer network security for the subsequent five years. The surveys stood three rounds comprising open-ended inquiry form and close-ended inquiry form, which were cast off to gather the opinions from an assembly of professionals. The fallout exemplifies the security of an organization's computer network these days and for the succeeding five years (2011-2015). To summarize, results designated the consequence of control, hardware, software and discretion, which are all essential to someone who is anxious about network security. This will afford the capacity to cope and switch the pertinent features to encounter the impending requirements and security concerns of an establishment's computer network. Wenjia Li and Anupam Joshi et al [8] strained to review the security disputes in the mobile ad hoc networks. Owing to the mobility and open media attitude, the mobile ad hoc networks are much more disposed to all benevolent to security jeopardize, such as information leak, interruption, or denial of service. Consequently, the security desires in the mobile ad hoc networks are considerably higher than those in the old-fashioned wired networks. Since the advent of the notion prevalent calculating, there is a snowballing requisite for the network consumers to get associated throughout the world every time by everywhere, which stimulates the occurrence of the mobile ad hoc network. Though, with the expediency that the mobile ad hoc networks have fetched to us, there are also amassed security threats for the mobile ad hoc network, which requisite for advance sufficient devotion. Al-Sakib Khan Pathan et al [9] decided that utmost attacks besides security for wireless sensor networks are instigated by the inclusion of false evidence by the conceded nodes within the network. For shielding the annexation of false information by conceded nodes, a means is vital for perceiving false information. Conversely, evolving such a discovery appliance and building it effectual embodies a prodigious research experiment. Yet again, endorsing complete security in a wireless sensor network is a key research subject. Lots of today's projected security systems are built on precise network prototypes. As present is a dearth of joined exertion to take a conjoint archetypal to safeguard security for every layer, in imminent, however, the security mechanisms grow into ingrained for each discrete layer, coalescing all the mechanisms together for creating them works in association with each other will sustain a firm research rebel. Though complete security could be warranted for wireless sensor networks,

the cost-efficacy and energy efficacy to employ such contrivances could still stance boundless research encounter.

Natarajan Meghanathan et al [10] deliberated that the nub behind network security is to guarantee admittance to the network and its data for certified hosts/users and repudiate admittance to illegitimate hosts/users. A protected network desires to have damage resistant communication means and buoyant decorum tools that can evade or condense the likelihoods of an attack. A close gaze at the orthodox network attacks divulges that IP spoofing has been behindhand with the triumph of these attacks. Therefore, it has become a design obligation in toting to validate the request users; it is also crucial to check the networks and hosts from which the request users are interactive in the Internet. Protocol contrivances like SSH, TLS, IPsec and Kerberos confirm that the above prerequisite is being taken care of and condense the odds of spoofing-based attacks. A solitary security regulatory contrivance cannot battle all varieties of network attacks. The security regulatory contrivance preferred for a network should be established on the precise threats that presently exist in the network. There is constantly a quid pro quo amid by security regulatory contrivance as sheer plug-in components and creating them further entrenched with the principal functionality of the protocols in the TCP/IP stack. It would be healthier for a security regulatory contrivance to necessitate vagaries to be made merely in one specific layer of the Internet protocol stack reasonably than all the layers. Keiko Hashizume, David G Rosado et al [11] alleged that much-deliberated security disputed about clouds devoid of building any variance concerning vulnerabilities and threats. However, they have absorbed on this discrepancy and substantial chief to appreciate these topics. Computing these security concerns was not sufficient; it thus prepared a connexion between threats and vulnerabilities to recognize what vulnerabilities subsidize to the performance of these threats and make the scheme healthier. Likewise, some present resolutions were recorded permitted to alleviate these threats. Though, new security methods are desired as well as reformed obsolete elucidations that can labour with cloud architectures. Outmoded security contrivances may not work fine in cloud atmospheres since it is a multifaceted design that is poised of a mishmash of dissimilar technologies. Virtualization permits several users to stake a physical server is one of the chief anxieties for cloud users. Likewise, added challenge is that there are diverse kinds of virtualization methods, and each methods line of attack of security appliances is different. Virtual systems are also bull's eye for some attacks exclusively when collaborating with distant virtual systems. Advisen insurance intelligence et al [12] recommended that though cyber risks are apparent as a hazard by supreme risk experts, executive directors, and board of directors, Asia-Pac businesses have been sluggish to espouse firm cyber risk management approaches. For instance, the threats connected to the practice of social media, cloud computing, and mobile devices are less probable to be perceived by Asia-Pac businesses than companies in North America and in Europe. Similarly, cyber threats are still essentially alleged as a staid delinquent by merely the leading establishments. In North America and Europe, smaller corporations currently opinion cyber risks as extremely if not more earnestly than their superior compliments where the opposed is factual for Asia-Pac enterprises. Utmost businesses privilege that network security risks are a detailed risk management emphasis with their instigation; most have not assimilated insurance as part upon the policy. Attention in buying the concealment also seems to be trifling.

Venkata Narasimha Inukollu et al [13] offered numerous security procedures, which would advance the security of cloud computing atmosphere. Subsequently, the cloud atmosphere is a combination of several dissimilar know-hows, projected numerous elucidations, which communally will create the atmosphere protected. Their elucidations inspire the usage of various skills/tackles to alleviate the security problem detailed. Security recommendations are intended such that they do not decline the efficacy and mounting of cloud schemes. Subsequent, security processes should be reserved to guarantee the security in a cloud atmosphere. Cloud environment is broadly recycled in business and research traits; hence security is a significant feature for establishments instigating on cloud environments. By projected methodologies, cloud atmospheres can be tenable for multifarious business dealings. Ahmed M. Al Naamany et al [14] aimed IEEE802.11 to interrelate wireless expedients to wired networks; the purpose was to realize networking with least or nope security. Security was not an imperative concern at that leg, conversely, with the prosperous WLANs and the reckless espousal of this method; security befitted significant and attaining security became a prime anxiety. Wired Equivalent Privacy (WEP) security protocols was the leading to be embraced in an effort to gratify the necessity for acquiring wireless networks, soon WEP grew into susceptible and there was a mandate for an improved security etiquette. Diligences already capitalized in wireless devices so some fresh protocol must reflect the hardware competences of such strategies. TKIP originated into the portrait with the intention of a healthy security in expending the similar hardware. Exaltation in software is what made TKIP more tenable than WEP. Conversely, the core encryption algorithm remains similar, feeble RC4 stream cipher blemishes it capabilities, TKIP supposed to be a small term resolution. IEEE documented the requisite for a novel protocol that is further locked and protracted. IEEE, in conclusion, replied the demand by operating on a novel security customary, IEEE802. 11i, the customary was accepted in June 2004. This original customary report fresh security protocols and familiarizes the acceptance of robust block encryption algorithm, Advanced Encryption Standard (AES),

also presents a new key organization pattern. Eric Ke Wang, S.M.Yiu et al [15] explored the security contests and glitches of Cyber-Physical Schemes and suggested a security framework for CPS. These challenges and issues bring enough motivation for future discussions and interests of research work on security aspects for CPS. Fadi Aloula, A R.Al-Alia et al [16] concluded that traditional power systems are moving towards digitally enabled smart grids which will enhance communications, improve efficiency, increase reliability, and reduce the costs of electricity services. The massiveness of the smart grid and the increased communication capabilities make it more prone to cyber-attacks. Since the smart grid is considered a critical infrastructure, all vulnerabilities should be identified and sufficient solutions must be implemented to reduce the risks to an acceptable secure level. They surveyed the vulnerabilities in smart grid networks, the types of attacks and attackers, the challenges present in designing new security solutions, and the current and needed solutions. Sen Xu, Manton Matthews et al [17] analyzed the vulnerability in authentication and key management protocols of 802.16. The revised protocols can prevent many kinds of attacks, such as replay attacks to BS and SS. They also proposed a security roaming protocol for 802.16e, which provides fast handover and guarantees backward and forward secrecy to some extent. The proposed mobility will bring up more problems in authentication and key management protocols and make them more vulnerable. Therefore, should pay more attention to the security issues in the drafts from TGe before they are approved as standards. Secure roaming in PKMv2 needs more works to finish. Mesh network in 802.16 also needs separate study. Multicast is another issue in the new standard, where authentication and key management protocols should be revised to facilitate the multicast functions.

Mohammad Hossein Manshaei et al [18] presented an overview of security and privacy problems that are analyzed within a game-theoretic framework. Reviewed and compared existing security games in computer networks in terms of players, game models, game-theoretic approaches, and equilibrium analysis. They further discussed some security protocols that are developed by mechanism design. The general objective is to identify and address the security and privacy problems, where game theory can be applied to model and evaluate security problems and consequently used to design efficient protocols. One of the main problems with modeling network security from the defense perspective is the lack of motivation that partly stems from the difficulty of quantifying the value added by network security. There is much confusion on how to assess and quantify network security. This lack of quantification naturally affects the decision making process regarding security investments. Security at network layer imposes future challenges to address security at a larger and more complex scale and game theory provides a preliminary tool that enables a quantitative study of such complex systems. Stefan Schmidt, Holger Krahn et al [19] proposed a security architecture that provides confidentiality, integrity, and authentication for a mobile wireless sensor network. Also presented algorithms to easily set up pairwise secret keys between the mobile sensor nodes and to establish a sending cluster per node, in which it can communicate its messages securely. Furthermore, our solution minimizes the effects of compromised nodes. Compromising an adjustable number of sensor nodes does not compromise the whole security architecture but restricts the security breach to the immediate neighbourhood of the compromised node. Implemented a prototype of security architecture, which clearly shows that it is a lightweight solution and applicable for self-organizing mobile wireless sensor networks. As a future direction, would like to integrate the ability to identify compromised nodes and methods to exclude them from the network. Another interesting question is to determine how much further we can optimize the employed algorithms with respect to memory usage and speed.

Mike Burmester, Yvo Desmedt et al [20] suggested that in order to preserve and affirm the liberties and freedoms that are at the core of our society it is therefore essential that we form a nucleus of new models, concepts, policies, tools, and techniques, to balance privacy and accountability. In a democratic society one must be able to speak freely, yet not be able to shelter threatening or deadly communications from proper authorities. At the same time, citizens should be able to adequately protect themselves; even from their own government should democracy dissolve or be overthrown. Everyone must be able to move about freely without tracked by a big brother, yet not be able to hide malicious actions from investigators as long as our society remains democratic. One must have reasonable access to goods, services, and information while protecting the rights of producers to earn a fair profit. Now is the time to set a course to establish a framework and the inner-workings to provide answerable privacy. An agency is needed to be designated to take the lead to establish a coordinated plan to improve and expand, but not restrict, security and privacy research and technology directions. Once this technology is in place, value decisions regarding privacy policies can be made by policy setters based on the best means for achieving the desired functionality, rather than being limited by the lack of options that presently exist. Sanjay goel and Stephen Bush et al [21] concluded that the security models for detection and elimination of pathogens that invade computer networks have been based on perimeter defense. Such defenses are proving inept against fast-spreading viruses and worms. The current tools are unable to guarantee adequate protection of data and unfettered access to services. It is imperative to complement these existing security models with reactive systems that are able to detect new strains of pathogens reliably and are able to destroy them before they can cause damage and propagate further. Several biological paradigms provide

a rich substrate to conceptualize and build computer security models that are reactive in nature. Three specific mechanisms in mammalian organisms present the most potential: (1) the RNAi mechanism, (2) protein pathway mapping, and (3) the immune mechanism. In addition, the models of disease control that study the spread and control of viruses suggest ways to throttle the spread of viruses. Current work has mainly focused on the use of immune and epidemiological models. It is time to move beyond these existing models to other innovative models, such as those based on genomics and proteomics. Such reactive models provide a scalable, resilient, and cost-effective mechanism that may keep pace with constantly evolving security needs. Virginia Horniak ae al [22] concluded that there are many ways to have a secure communication in computer networks today. Today there are both possibilities to encrypt the data that is transmitted in a computer network and possibilities to control which users have authority to use network systems. Both encryption and authentication have algorithms and protocols that have been or are widely used. Along with the computer security there are ethical questions that come up. Authorities are concerned over the fact that encrypted communication over computer networks can be misused by terrorists and other criminals and therefore the legislation in many countries around the world has come into force. Civil rights organizations mean that the right to communicate with each other using encryption is a civil right. The legislation is by many found to be a violation of a person's right to privacy. Waiting for the next generation of privacy-protected technology, where there will be no one who feels that the technology in combination with the legislation is a violation of human right to privacy, it is important that the industry adopts a more universal and ethical approach towards privacy.

Dragan Pleskonjic, Nemanja Macek et al [23] really tried not to push readers with maths in cryptography; instead, told the readers that it is important part of their computer software and to show them how they can use it for free. To teach the readers that money does not necessarily buys a good security mechanisms – a good firewall can be set up with $100 computer running Linux and iptables. This is a comprehensive manual that serves the protectors, not a hacker's handbook; if you are looking for malicious recourses, suggest you to try somewhere else. Their book was the first systematic computer security book in Serbian language. Salah Alabady et al [24] discussed the security weakness in router and firewall configuration system and risks when connected to the Internet .Also presented the tips and recommendations to achieve a best security and to protect the network from vulnerabilities, threats, and attacks by applying the security configurations on router and firewall. Also one can use this suggested security policy as a checklist to use in evaluating whether a unit is adhering to best practices in computer security and data confidentiality. The firewall provides additional access control over connections and network traffic and perform user authentication. Using a firewall and a router together one can offer better security than either alone. A poor router filtering configuration can reduce the overall security of a network, expose internal network components to scans and attacks.

Sarvesh Tanwar, Prema et al [25] suggested that one can see that attacks against the ad hoc networks may vary depend on (1) which environment the attacks are launched, (2) what communication layer the attacks are targeting, and (3) what level of ad hoc network mechanisms are targeted. One can also see that there are several attack characteristics that must be considered in designing any security measure for the ad hoc network. Due to nature of mobility and open media MANET are much more prone to all kind of security risks as covered. As a result, the security needs in the MANET are much higher than those in the traditional wired networks. They designed the new model of security which can handle these attacks. For security purpose, all the nodes are authenticated by using the Digital Certificate or Digital Signature. By providing authentication malicious node can't enter the network. IEEE Computer society et al [26] concluded that with the Internet's growth and the corresponding increase in computer related crime, it is essential and inevitable that CNF training and education programs will appear. Hope and intent that these programs will not be developed in a vacuum or without thought of how best to form a global CNF workforce. The opportunity is great. Like television, computing has permeated society very quickly and with a dramatic impact. Unlike television, though, computing technology is a prime target and tool for criminals because of its interactive nature, ability to store important information, and use in commerce. Presently, computing forensics training is provided almost exclusively by law enforcement organizations; only a few universities support computing forensics programs, and most comprise only one course. Expect this to change over the next three to five years, and hope that evolving programs can leverage experience gained through the recent US National Security Agency-prompted expansion of information-assurance education programs. The health of the Internet itself may depend on it.

Donald Graji, Mohnish Pabrai et al [27] examined a possible methodology for network security design and attempted to apply it to a simple application. It was found that several pitfalls await the requirements specifier. One problem is that defining and classifying security services is not as straightforward as one would like. Different parts of the network, for example, may have differing needs. They observed that it is not always easy to separate security mechanisms from security protocols, and certainly both need to be considered in proofs of correctness. A more fundamental criticism of the methodology is its rigid sequencing of specification followed by design followed by implementation. Sometimes, subparts of the overall problem are found to be so large that all the steps of the method must be reapplied to that subpart. For example, providing a more desirable

solution to the problem of managing public keys within the XYZ Corporation may require application of the complete methodology, beginning again at the specification stage. It may be that the methodology is insufficiently adaptable to rethinking or changes occurring during the design process. Sriram Natarajan and Tilman Wolf et al [28] concluded that Network virtualization has received significant attention in recent years. They argued that it is important to consider the security issues and vulnerabilities in the virtualized networks since their architecture is fundamentally different from the current Internet. Their work has identified potential attacks and presented some initial ideas on how to develop suitable defense mechanism. They believed that their observations provide an important first step toward a more detailed understanding of solutions to secure network virtualization in the future Internet. Alec Yasinsac, Yanet Manzano et al [29] described that computer related crime is growing as fast as the Internet itself. Today, enterprises focus on implementing preventative security solutions that reduce vulnerabilities, with little concern for systematic recovery or investigation. They proposed six categories of policies that will enable or facilitate after-the fact action that can reduce the impact of computer crime and can deter computer crime from occurring. Some of the policies that they proposed were simple actions that responsible network managers already engage as a matter of system reliability or as part of disaster recovery procedures. The focus on computer and network forensics distinguishes these policies from backup and recovery needs. The procedures for CNF require systematic application and detailed documentation; else the information may not be admissible in court. Further, backup and recovery procedures routinely ignore temporary information and other important sources of potential evidence.

Haowen Chan and Adrian Perrig et al [30] suggested that the proliferation of sensor networks will inevitably extend to criminals who can use them for illegal purposes. For example, thieves can spread sensors on the grounds of a private home to detect the inhabitants' presence. If the sensors are small enough, they can also plant them on computers and cell phones to extract private information and passwords. With widespread use, the cost and availability barriers that discourage such attacks will drop. Sensor detectors offer one possible defense against such attacks. A detector must be able not only to detect the presence of potentially hostile wireless communications within an area that may have significant levels of radio interference but also to differentiate between the transmissions of authorized and unauthorized sensor networks and other devices. Such technologies might not prevent unauthorized parties from deploying sensor networks in sensitive areas, but they would make it more costly, thus alleviating the problem somewhat. Sensor networks are set to become a truly pervasive technology that will affect our daily lives in important ways. They insisted that cannot deploy such a critical technology, however, without first addressing the security and privacy research challenges to ensure that it does not turn against those whom it is meant to benefit. Joseph V. Antrosio and Errin W. Fulp et al [31] introduced a new malware defense system consisting of three basic components: security authentication, quarantine system, and the policy manager. Security authentication is an effective and anonymous method to ensure the safety of hosts on a network. In contrast to user authentication, security authentication detects and characterizes the vulnerabilities of the machine in question. This new type of authentication is necessary since an authenticated user can bring a vulnerable or infected machine into a secure network. Therefore, the system is particularly effective at preventing the spread of malware inside a local network (e.g. mobile environment) where traditional firewall systems are no longer effective. Furthermore, the proposed defense is not restricted to a certain instance of malware since vulnerabilities are targeted instead of fingerprints. Security authentication credentials are used by the policy manager to quarantine the machine. The quarantine system isolates the machine by placing them in a security cell, which utilizes the network and MAC layers to prevent the machine from being infected or attacked by other hosts and vice versa. Unlike current systems that disconnect a suspect machine, the quarantine system affords the machine a certain level of network connectivity. This allows the machine to still function until the malware or vulnerability is addressed. This paper also discussed how the proposed system can be applied to TCP/IP networks utilizing current network technology and tools. Advanced routing and VLAN's offer the necessary quarantine abilities, while Nessus and Nmap are sufficient for simple security authentication. The proposed malware defense was successfully implemented and tested using these tools and basic Linux equipped computers.

B V Ramana Murthy, Vuppu Padmakar et al [32] concluded that the risks to users of wireless technology have increased as the service has become more popular. Hackers had not yet had time to latch on to the new technology and wireless was not commonly found in the work place. However, there are a great number of security risks associated with the current wireless protocols and encryption methods, and in the carelessness and ignorance that exists at the user and corporate IT level. Hacking methods have become much more sophisticated and innovative with wireless. Hacking has also become much easier and more accessible. Windows or Linux-based tools were made available on the web at no charge. Some organizations that have no wireless access points installed do not feel that they need to address wireless security concerns. In-Stat MDR and META Group have estimated that 95% of all corporate laptop computers that were planned to be purchased in 2005 were equipped with wireless. Issues can arise in a supposedly non-wireless organization when a wireless laptop is plugged into the corporate network. A hacker could sit out in the parking lot and gather info from it

through laptops and/or other devices as handhelds, or even break in through this wireless card equipped laptop and gain access to the wired network. Rangarajan Athi Vasudevan et al [33] illustrated a method of implementing message authentication by private key without the exchange of any more information. The concept of the one-time pad is implemented in the course of the algorithm resulting in information-theoretic security of data transfer. The issue of key management is addressed by firstly the exchange of a large number a priori, and then subsequent modifications to the large number at regular intervals. These modifications are designed such that their outputs seem random to the adversary. Also, flexibility in the form of a means of control is provided in the algorithm to monitor and check the overhead resulting because of the data expansion due to the arbitrary splitting. Trade-offs involved in the practical realization of the algorithm have been discussed and their relative impacts on the performance analyzed. Also suggested a technique to make the algorithm secure against cryptanalytic attacks in the eventuality when the nature of the data is revealed. The inclusion of this has been proved to still be substantially more efficient than encryption algorithms. Moreover, realization of the "jigsaw" paradigm has been designed to support a parallel implementation catering to future technological advancements.

M. Milton Joe et al [34] concluded that online social networking applications are mostly used by all the people in and around the world. Most of the time of a day is spent in online social networking applications. However, the users of online social networks are unaware of the security issues do exist in OSN platform. There are various security issues which steals the sensitive and personal information of a user. Their paper illustrated the various security issues available in online social networks. The future direction of the research will be modelling effective security algorithms to defend the security issues exist in online social networks. Bhavya Daya et al [35] reported that the security threats and internet protocol were analyzed to determine the necessary security technology. The security technology is mostly software based, but many common hardware devices are used. The current development in network security is not very impressive. Originally it was assumed that with the importance of the network security field, new approaches to security, both hardware and software, would be actively researched. It was a surprise to see most of the development taking place in the same technologies being currently used. The embedded security of the new internet protocol IPv6 may provide many benefits to internet users. Although some security issues were observed, the IPv6 internet protocol seems to evade many of the current popular attacks. Combined use of IPv6 and security tools such as firewalls, intrusion detection, and authentication mechanisms will prove effective in guarding intellectual property for the near future. The network security field may have to evolve more rapidly to deal with the threats further in the future. Giannis F. Marias1, Joao Barros et al [36] identified security and privacy issues for the Network of the Future (NF). They focused on recent achievements on network security, in physical and network layers. Emphasized on virtualization, cognitive radio and information-centric future networks, that is, on today's communication and networking paradigms that are foreseen as future network components. They discussed the necessity and the challenges of global authentication and identity management for the NF; privacy issues and the required privacy enhancements on the future Internet. They further concentrated on challenges and the state-of-the-art of measuring security and privacy in the NF. They finally addressed mobile applications' security and privacy. The research in the area is ongoing, but promising results are already well motivated.

Yang Xiao, Chaitanya Bandela et al [37] introduced the security issues in the IEEE 802.11 WLANs and premeditated two enhancements for the WEP. They led simulations/experiments on comparisons of these schemes with the original WEP scheme. The proposed enhancements provide better data confidentiality with some degree of computing cost as the trade-off. The improved schemes overcome the weaknesses resulting from Key Sequence Reuse. They make use of not only the varying IV states, but also varying key states in order to supply a higher seed space resulting in lesser key stream reuse. It is not easy to mount decryption dictionary attacks, since the total number of key streams to be discovered increases largely relative to the WEP and the key streams used change from day to day for the same IV. Key Management is partially solved since the system is not easily compromised despite the secret key remaining unchanged for a long time. Message Tampering is completely avoided from the use of Keyed Message Authentication mechanism. Security against Message Injection is heightened since discovery of a key stream is useful to the intruder only until the next session key change. If session key is refreshed frequently enough, depending on the network traffic, the vulnerability can be kept under check. Authentication spoofing is made difficult by using Kerberos based authentication. Dharma P. Agrawal, Hongmei Deng et al [38] suggested that mobile computing technology provides anytime and anywhere service to mobile users by combining wireless networking and mobility, which would engender various new applications and services. However, the inherent characteristics of wireless communication and the demand for mobility and portability make mobile computing more vulnerable to various threats than traditional networks. Securing mobile computing is critical to develop viable applications. In their article, discussed the security issues faced by mobile computing technology analysed the various security threats and describe the existing current countermeasures. Many security solutions have been proposed to securing WLANs, but no one is able to claim that it solves all the security problems, or even most of them. In essence, secure mobile computing would

be a long-term ongoing research topic. Farzad Sabahi et al [39] suggested that way for decentralized application and access every time and everywhere to data, occasion and introduce new set of challenges and security problems that must consider before transfer data to a cloud environment. Additionally, just because the software can run in a Virtual machine does not mean that it performs well in cloud environment necessarily. Thereupon, in cloud there are risks and hidden costs in managing cloud compliance. The key to successful cloud computing initiatives is achieving a balance between the business benefits and the hidden potential risks which can impact efficacy. Cloud providers often have several powerful servers and resources in order to provide appropriate services for their users but cloud is at risk similar to other Internet-based technology. In the other hand, they are also at risk of attacks such as powerful DDoS attacks similar other Internet-based technology. As a solution, cloud providers can add more resource to protect themselves from such attacks but unfortunately there is no defense against a powerful DDoS attack which has good sapience. These issues which discussed in this paper are the main reasons that cause many enterprises which have a plane to migrate to cloud prefer using cloud for less sensitive data and store important data in their own local machines. Ming li and Wenjing Lou et al [40] summarized that ABE-based access control method is more capable than other techniques of achieving all the security requirements. It is fine-grained, context-aware, revocable, and efficient to implement on local servers. However, the above mentioned schemes have not satisfactorily addressed the security-safety conflict. Since it is important to allow on-demand access policy adaptations during emergency healthcare, a future direction is to design more flexible, cryptographic enforced, and attribute based access control schemes for WBANs. The WBAN is an emerging and promising technology that will change people's healthcare experiences revolutionarily. Data security and privacy in WBANs and WBAN-related e-healthcare systems is an important area, and there still remain a number of considerable challenges to overcome. The research in this area is still in its infancy now, but we believe it will draw an enormous amount of interest in coming years. We hope this article will inspire novel and practical designs of secure, dependable, and privacy enhanced WBANs.

III. Conclusions

Computer networking has developed copiously and entrenched in our communal drapery in diminutive time duration. Conglomerates that are arriving in this milieu these days rely on the security and privacy of the computer network. Subsequently, the safekeeping and solitude of these networks befits a perilous aspect to be corporate, on top of the common user. In this broadsheet, accounting to the attacks that already exist, there are sanctuary trials and contemporary isometrics envisioned to mend security and ease jeopardizes, thus mustering the atmosphere innocuous to the users. The utmost shared contemporary isometric of computer network and security is enumerated beneath;

Metric 1: Standard Guards Analysis (Antivirus, Antispyware, Firewall)

This is a quantity of exactly how fine you are shielding your wits beside the utmost elementary security threats. Your analysis of diplomacies by these security outfits should be in the choice of 94% to 98%. Less than 90% reportage may be the root for distress. You can recap the network scan at consistent interludes to perceive if attention is tumbling or plot firm.

Metric 2: Patch Potential

Patch-potential is the stint flanked by a patch's proclamation and your efficacious disposition of those patches. It is a display of a corporation's patching chastisement and capability to respond to feats. As with standard guard metrics, patch potential prominence may illustrate systems with heaps of absent patches or systems with archaic patches, which may plug to the necessity for integrated patch supervision or progression enhancements that might evade the system from utmost susceptible to spasm.

Metric 3: Watchword Clout

This metric compromises modest risk decline by sieving out wicked watchwords and building them stiffer to disruption, and discovering possible feeble acnes where main systems use defaulting watchwords. Password blowing can also be an influential carnival tool with officials who possess frail watchwords. By representing them in person how rapidly you can blow their watchword, you will progress your streaks of connexion with them and their indulgent of your starring role.

Metric 4: Platform Obedience Records

Commonly accessible tools, such as the Centre for Internet Security (CIS) tot up toolset, can run checks against systems to catch out if your hardware encounters top exercise morals such as those established by CIS. The software gears take lesser time to run and check such effects as the ports are given up gratuitously exposed, systems are arbitrarily shared; default approvals are given up and other standards but frequently ignored security gaps.

Metric 5: Candid E-Mail Traffic Probe

Candid E-Mail Traffic Probe is kinfolk of isometric counting inward and outbound traffic capacity as well as magnitude and traffic stream between your business and others. Here are frequent means to analyses this data; scheming the communize drift between your business, and your contestants may be vigilant you to a worker revealing intellectual property.

References

[1] Mahfuzulhoq Chowdhury, Md Fazlul Kader and Asaduzzaman, "Security Issues in Wireless Sensor Networks: A Survey", International Journal of Future Generation Communication and Networking, Vol.6, No.5, 2013, pp.97-116.

[2] Sattarova Feruza Y and Prof.Tao-hoon Kim, "IT Security Review: Privacy, Protection, Access Control, Assurance and System Security", International Journal of Multimedia and Ubiquitous Engineering, Vol. 2, No. 2, April, 2007, pp.17-32.

[3] Robert Koch, Bjorn Stelte, Mario Golling, "Attack Trends in Present Computer Networks", 4th International Conference on Cyber Conflict, C. Czosseck, R. Ottis, K. Ziolkowski (Eds.), NATO CCD COE Publications, Tallinn, 2012, pp.269-280.

[4] Di Ma, Gene Tsudik, "Security and Privacy in Emerging Wireless Networks", IEEE Wireless Communications, October 2010, pp.12-21. http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5601953

[5] Wenye Wang, Zhuo Lu, "Cyber security in the Smart Grid: Survey and challenges", Computer Networks 57, Elsevier, 2013, pp.1344–1371, http://dx.doi.org/10.1016/j.comnet.2012.12.017

[6] Gurveen K.Sandhu, Gurpreet Singh Mann, Rajdeep Kaur, "Benefit and security issues in wireless technologies: Wi-fi and WiMax", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 1, Issue 4, June 2013, pp.976-982.

[7] Cholatip Yawut, Phattarapong Keawpipop, "The Future of Organization's Computer Network Security for the Next 5 Years (2011-2015) by Using Delphi Technique", International Conference on Information and Electronics Engineering, vol.6, 2011, IACSIT Press, Singapore, pp.184-188.

[8] Wenjia Li and Anupam Joshi, "Security Issues in Mobile Ad Hoc Networks - A Survey", http://www.csee.umbc.edu/~wenjia1/699_report.pdf

[9] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges", ISBN 89-5519-129-4, Feb. 20-22, 2006 ICACT2006, pp.1043-1048, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1625756&tag=1

[10] Natarajan Meghanathan, "A Tutorial on Network Security: Attacks and Controls", http://arxiv.org/ftp/arxiv/papers/1412/1412.6017.pdf

[11] Keiko Hashizume, David G Rosado, Eduardo Fernandez-Medina, Eduardo B Fernandez, "An analysis of security issues for cloud computing", Journal of Internet Services and Applications 2013, 4(5), Springer, pp.1-13, http://www.jisajournal.com/content/4/1/5

[12] Advisen Insurance Intelligence, "A survey of enterprise-wide cyber risk management practices in the asia-pacific region ", Network security and cyber risk management, April 2014, Zurich. http://www.advisenltd.com/research/white-papers/2014-network-security-cyber-risk-management-survey-enterprise-wide-cyber-risk-management-practices-asia-pacific-region/

[13] Venkata Narasimha Inukollu, Sailaja Arsi and Srinivasa Rao Ravuri, "Security issues associated with big data in cloud computing", International Journal of Network Security & Its Applications, Vol.6, No.3, May 2014, pp.45-56, DOI: 10.5121/ijnsa.2014.6304.

[14] Ahmed M. Al Naamany, Ali Al Shidhani, Bourdoucen, "IEEE 802.11 Wireless LAN Security Overview", International Journal of Computer Science and Network Security, Vol.6 No.5B, May 2006, pp.183-156.

[15] Eric Ke Wang, Yunming Ye, Xiaofei Xu, S.M.Yiu, L.C.K.Hui, K.P.Chow, "Security Issues and Challenges for Cyber Physical System", IEEE/ACM International Conference on Cyber, Physical and Social Computing, 2010 IEEE, pp.733-738, DOI 10.1109/GreenCom-CPSCom.2010.36

[16] Fadi Aloula, A. R. Al-Alia, Rami Al-Dalkya, Mamoun Al-Mardinia, Wassim El-Hajjb, "Smart Grid Security: Threats, Vulnerabilities and Solutions", International Journal of Smart Grid and Clean Energy, vol. 1, no. 1, September 2012, pp.1-6.

[17] Sen Xu, Manton Matthews, Chin-Tser Huang, "Security Issues in Privacy and Key Management Protocols of IEEE 802.16", ACM SE'06, March 10-12, 2006, Melbourne, Florida, USA.

[18] Mohammad Hossein Manshaei, Quanyan Zhu, Tansu Alpcan, Tamer Basar, Jean-Pierre Hubaux, "Game Theory Meets Network Security and Privacy", EPFL Technical Report-151965, September 2010, http://publish.illinois.edu/quanyanzhu/files/2012/10/ACMSurvey.pdf

[19] Stefan Schmidt, Holger Krahn, Stefan Fischer, and Dietmar Watjen, "A Security Architecture for Mobile Wireless Sensor Networks", ESAS 2004, LNCS 3313, pp. 166–177, Springer-Verlag Berlin Heidelberg, http://link.springer.com/chapter/10.1007%2F978-3-540-30496-8_14

[20] Mike Burmester, Yvo Desmedt, Rebecca Wright, Alec Yasinsac, "Security or Privacy, Must We Choose?" http://www.cs.fsu.edu/~yasinsac/Papers/BDWY01.pdf

[21] Sanjay Goel and Stephen Bush, "Biological models of security for virus propagation in computer networks", Login, Vol. 29, No. 6, December 2004, pp.49-56.

[22] Virginia Horniak, "Computer Security and Ethics", http://www.idt.mdh.se/kurser/cd5590/Archives/07_11/

[23] Dragan Pleskonjic, Nemanja Macek, Borislav Dordevic, "Security of Computer Systems and Networks", ComSIS Vol. 4, No. 1, June 2007.

[24] Salah Alabady, "Design and Implementation of a Network Security Model for Cooperative Network", International Arab Journal of e-Technology, Vol. 1, No. 2, June 2009, pp.26-36.

[25] Sarvesh Tanwar, Prema KV,"Threats & Security Issues in Ad hoc network: A Survey Report", International Journal of Soft Computing and Engineering, Volume-2, Issue-6, January 2013, pp.138-143.

[26] Alec Yasinsac, Robert, Donald G.Marks, Mark M.Pollitt, Peter M.Sommer, "Computer Forensics Education", IEEE Security and Privacy, Published by the IEEE Computer Society, 2003, pp.15-23, http://computer.org/security/

[27] Donald Graji, Mohnish Pabrai, Uday Pahrai, "Methodology for Network Security Design", IEEE Communications Magazine, November 1990, pp.52-58.

[28] Sriram Natarajan and Tilman Wolf, "Security Issues in Network Virtualization for the Future Internet", http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6167481&tag=1

[29] Alec Yasinsac, "Policies to Enhance Computer and Network Forensics", Proceedings of the 2001 IEEE Workshop on Information Assurance and Security United States Military Academy, West Point, NY, 5-6 June, 2001, pp.289-295.

[30] Haowen Chan and Adrian, "Security and Privacy in Sensor Networks", October2003, pp.99-101, http://www.netsec.ethz.ch/publications/papers/ieee-secure-sensor-nets.pdf
[31] Joseph V. Antrosio, Errin W. Fulp, "Malware Defense Using Network Security Authentication", Proceedings of the IEEE International Information Assurance Workshop, 2005, pp.1-13.
[32] Dr.BV Ramana Murthy, Prof. Vuppu Padmakar, Ms.A.Vasavi, "Significances and Issues of Network Security", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 6, June 2014, pp.6922-6929.
[33] Rangarajan Athi Vasudevan, Ajith Abraham, Sugata Sanyal "A Novel Scheme for Secured Data Transfer over Computer Networks", http://www.tifr.res.in/~sanyal/papers/Ranga_SecuredDataTransfer.pdf
[34] M.Milton Joe, Dr. B.Ramakrishnan, "A Survey of Various Security Issues in Online Social Networks", International Journal of Computer Networks and Applications Volume 1, Issue 1, November – December, 2014, pp.11-14.
[35] Bhavya Daya, "Network Security: History, Importance, and Future", http://web.mit.edu/~bdaya/www/Network%20Security.pdf
[36] Giannis F. Marias, Joao Barros, Markus Fiedler, "Security and privacy issues for the network of the future", Security Comm. Networks, 2011, John Wiley & Sons, Ltd. 3.
[37] Yang Xiao, Chaitanya Bandela, "Security mechanisms, attacks and security enhancements for the IEEE 802.11 WLANs", Int. J. Wireless and Mobile Computing, Vol. 1, Nos. 3/4, 2006, pp.276-288.
[38] Dharma P. Agrawal, Hongmei Deng, Rajani Poosarla, "Secure Mobile Computing", http://link.springer.com/chapter/10.1007%2F978-3-540-24604-6_26#page-1
[39] Farzad Sabahi, "Cloud Computing Security Threats and Responses", 978-1-61284-486-2/111, 2011 IEEE, pp.245-249, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6014715&tag=1
[40] Ming li and Wenjing Lou, "Data Security and Privacy in Wireless Body Area Networks", IEEE Wireless Communications, February 2010, pp.51-58.

Biography

Dr.P.S.Jagadesh Kumar, Professor in the Department of Computer Science and Engineering, Don Bosco Institute of Technology, Bengaluru has 16 years of teaching experience, counting six years of research mania on the field of image compression, network security and cryptography. He received his B.E degree from University of Madras in Electrical and Electronics Engineering discipline in the year 1999. He obtained his M.E degree in 2004 with specialization in Computer Science and Engineering from Annamalai University, Chidambaram and his Ph.D. in digital image compression from Anna University, Chennai in 2014. He is a recipient of two best teacher awards, one young scientist award. He has two patents to his credit in the area of image compression and neural networks. He is one of the well-known academicians and researcher. He serves as the journal referee in many reputed journals and also as the editorial board member.