International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Vol. 12 Issue 12, December, 2023, Impact Factor: 7.751

Examining Hybrid Security Approach for Detecting and Preventing DOS and DDOS Attacks in Cloud Environments

Ajitesh Kumar Saha[1], Dr. Akash Saxena[2]

[1]Research Scholar, Department of Computer Science& Engineering, Mansarovar Global University, Sehore, Madhya Pradesh
[2]Supervisor, Department of Computer Science &Engineering, Mansarovar Global University, Sehore, Madhya Pradesh

ABSTRACT

With its scalability, flexibility, and cost-efficiency, cloud computing has completely changed how companies access and use computer resources. But new problems have also emerged as a result of this paradigm change, most obviously in the area of security. Cloud services are vulnerable to distributed denial of service (DDoS) and denial of service (DoS) attacks, which can disrupt service and compromise data. Protecting against denial-of-service (DoS) and distributed denial-of-service (DDoS) assaults is just the beginning; our proposed hybrid security architecture can also identify such attacks and sound an intrusion warning. Moving on from a review of previous solutions to the current one, the study suggests a hybrid paradigm as the best way forward. Every request that is created will be checked and filtered by the suggested hybrid model. Users will get answers once the system has monitored and filtered their request behavior. In addition to achieving availability services, the suggested approach will also reduce processing time and bandwidth utilization. By taking use of the elastic and scalable nature of cloud infrastructure, the hybrid method can assign resources dynamically and react to new threats as they arise in real-time, making it very successful in dynamic threat environments.

Keywords: Hybrid, Cloud computing, Security, Bandwidth, Attack

INTRODUCTION

On demand access to a wide range of computer resources, including data storage, networking, servers, analytics, intelligence, and software, is made possible over the internet through cloud computing. Paying for services is usually limited to what we actually use. Catering to the service requirements of a rapidly expanding sector is no easy feat. When in-house resources aren't enough, it's necessary to take use of the appealing services offered by cloud providers.

Services such as Platform as a service (PaaS), Software as a service (SaaS), and Infrastructure as a service (IaaS) are common in cloud computing. No one cloud, however, can meet the needs of every single client since no two clouds are alike. Consequently, a wide range of services are mushrooming to meet the demands of every business.

Businesses are increasingly embracing the cloud's on-demand, elastic, and accessible computing capabilities, and migrating their databases and apps there. Software-Defined Networking (SDN), another revolutionary idea in Internet design, also emerges around this period. Network function virtualization (SDN) is intended to resolve the complex network administration that now impedes the evolution of the Internet, while cloud computing makes it easier to manage computer and storage resources. In addition to being considered for the next generation of Internet architecture, software-defined networking (SDN) has already found its way into corporate data centers at Google and other IT corporations. There will soon be an era where SDN and cloud computing work together to provide IT services to enterprises.

A hybrid cloud allows users to easily transfer data and applications across multiple cloud providers by combining different types of cloud infrastructure using proprietary and standardized technologies. It would be a mistake to think of a simple combination of cloud and on-premise data as a hybrid cloud. In addition, it has to have these features:

- Delegation of tasks based on mobility.
- Connecting devices and systems across a local area network (LAN), wide area network (WAN), or virtual private network (VPN).
- Implementation of an all-inclusive unified automation platform.

- To hide the underlying facts, you need a sophisticated and strong middleware.
- Making use of resources that are both available and scalable.
- Combining plans for response and recovery from disasters.

It allows customers to expand their business by utilizing the appealing features of public cloud while safeguarding sensitive data with private cloud. Hybrid cloud is the optimal choice for businesses experiencing rapid fluctuations in demand, such as unexpected peaks or drops, due to its adaptability. Organizations can utilize public cloud services without granting direct access to their on-premise data centers. Business important data and apps may be securely stored while utilizing the computational power of the public cloud for difficult operations. Organizations will only pay for the services they use, without having to invest in procuring, developing, and maintaining additional resources that may be utilized for a short period and then remain unused for a long time. Private cloud is similar to public cloud but is often deployed in a client's data center and emphasizes self-service and scalability. The nature of single tone service, service-level agreement (SLA), and similar connections enhance the client-cloud interaction by making it more robust and less burdensome.

In addition to the often acknowledged advantages, the integration of cloud computing with SDN might potentially pose dangers, particularly in terms of network security. We will begin by examining Denial-of-Service (DoS) attacks, which are a common network security issue. DoS and DDoS attacks aim to render a service inaccessible to its intended consumers by depleting system or network resources. Despite decades of dedicated efforts by network security specialists, DDoS assaults persist in increasing in frequency and damage. Current DDoS attack protection solutions operate under the assumption that the network is completely controlled by business network managers. Thus, network managers have the option to install certain hardware components within the network to identify or lessen the impact of DDoS assaults. Yet, given the evolving network model of cloud computing and SDN, these assumptions are no longer valid.

REVIEW OF LITERATURE

Mbah, Thierry (2022)Cyber security is a dynamic field where attackers continuously create new methods to breach businesses' systems and data. Public and corporate businesses are facing challenges in protecting their systems and data from the ever-changing, advancing, and enduring threats. It is essential for both company and government organizations to safeguard their systems and data from possible dangers in order to ensure business or organizational continuity. Cyber thieves frequently focus on networks to carry out attacks on specific systems within organizations, aiming to obtain access and either steal, change, or destroy valuable data. These assaults may involve Malware, DDoS, SQL injection, Phishing, XSS, Botnets, and other forms of cyber threats. Cloud adoption has fundamentally altered the method by which programs are provided and utilized. Conventional networks do not have the necessary security and performance features to meet the demands posed by modern cloud issues. This research suggests a framework equipped with integrated algorithms for identifying both novel and pre-existing security risks. The study starts by analyzing the issues faced by intelligent networks. The second portion examines previous research conducted on cybersecurity in networks. The final section presents an architectural design that includes an embedded algorithm for identifying emerging network hazards. The final section focuses on implementing the architecture.

Garg, Deepak et al., (2022) The distributed creation of Cyber-Physical Systems (CPSs) for smart businesses has been made possible by new technological advances and industry trends. Due to data storage on cloud servers, which presents several limitations owing to the diverse nature of the devices engaged in communication, CPSs are mostly based on the Internet of Things (IoT). When it comes to the obstacles that slow down the progress of CPS realization, security is at the top of the list. Due to their inaccessibility from outside networks, designers presume that CPSs are inherently secure. On the other hand, modern CPSs incorporate elements of both the cyber and physical layers. Thus, due to the interconnected and physically present nature of the systems, complex industrial applications (CIA) pose significant cyber security risks to commercial critical infrastructure systems. In light of this, this work proposes Dynamic Hybrid Secured Encryption Technique (DHSE), a new data security technique that combines AES, IBE, and ABE with a hybrid encryption scheme. The data is categorized into three levels of sensitivity by the suggested algorithm: low, medium, and high. The names are labelled to produce named-data packets (NDPs), which are then used to disseminate the data. For 128-bit keys in DHSE, a minimum of 10 rounds are required, while the exact number of rounds can be adjusted according to the key size. For example, 3.25 ms is the average time it takes for Advanced Encryption Standard (AES), 2.18 ms for Identity-based encryption (IBE), and 2.39 ms for Attribute-Based Encryption (ABE). In contrast, other encryption methods take far longer than the average duration of 2.07 ms used by DHSE. The average decryption timings for AES, IBE, and ABE are 1.77 ms, 1.09 ms, and 1.20 ms, respectively, whereas the average durations for the DHSE decryption methods are 1.07 ms, significantly lower than those of other algorithms. Data confidentiality is ensured with minimal encryption and decryption time, according to the investigation, which also demonstrates that the framework is well-designed. Consequently, CPS-IoT is an ideal fit for the suggested method Roy, Prince &Gujral, Rajneesh (2021) The "pay as you go model" is utilized by cloud computing in order to supply its consumers with on-demand services, particularly those pertaining to data storage, computing power, network, and other related services. Over the course of the past several years, Cloud Technology, which is a decentralized network, has emerged as one of

the most effective methods for storing and processing excessive amounts of data. The storage and processing of data via cloud networks is accomplished through the achievement of security in terms of authentication, integrity, and privacy, which is a significant difficulty in the modern world. This study had presented a Multilevel level hybrid security framework with the purpose of preserving security via the utilization of session key generation, cryptography algorithms, chain of hashes, and the storage of data through the use of decentralized ways such as BlockChain. This framework protects all of the security services and reduces the amount of passive and active assaults, including modifications, fabrications, hijacking of sessions, network jamming, denial of service attacks, and efforts to change or manipulate pathways in order to get access.

Anjaliet al., (2021) To effectively manage the risks associated with cloud computing, it is essential to have a solid understanding of the nature of the security risks. The efforts that have been made by both the academic community and the technological community, such as ENISA, CSA, and NIST, to investigate security risks and vulnerabilities associated to cloud systems are proof of the significance of security issues. The provisioning of secure virtual networks (SVNs) in an environment with many tenants is an essential component in order to guarantee confidence in public cloud systems and to support the development of these systems. Nevertheless, comparing findings that are SVN-oriented is a challenging task since there are not enough studies that provide a full list of dangers that such results should cover and that brief the primary businesses that are involved in network virtualization. This study proposes a threat category for cloud networking in order to solve this issue. It does so by providing threat classes and attack scenarios that have to be taken into consideration while creating, comparing, or categorizing outcomes. This classification is based on the CSA difficulty report, which is based on research and checks from the technical literature. The purpose of this classification is to broaden the list of risks and provide a complete analysis of cloud network virtualization concerns.

Ferdous, Jannatul et al., (2020) Deciphering the Daily Computing Issues requires an understanding of the notion of cloud computing. In essence, it is a digital repository of resources, and it also makes these tools available to clients over the internet. It is an innovation that is dependent on the internet and is employed in computer technology. Information privacy, protection, anonymity, reliability, and other issues with cloud computing are among the most frequent problems associated with this technology. On the other hand, the most important concern pertains to security and the manner in which the cloud provider assures it. It is necessary to ensure the safety of both the treatments (calculations) and the storage (databases) that are hosted by the cloud provider in order to safeguard the cloud. The document provides a survey of parallel works that discuss the topic of cloud computing security. Through conducting research, we have been able to identify and analyze a variety of security issues that are associated with the cloud. Additionally, we have identified and analyzed a number of cryptographic algorithms that are adaptable to better security for the cloud. Based on these algorithms, we have proposed a hybrid framework for security in cloud computing.

Farnga, Max (2018) Despite the fact that cloud computing offers lower infrastructure costs, increased agility, and faster delivery, it also poses higher operational and security risks for business critical assets. However, a solution and security architecture that are well designed will ensure that businesses remain safe both during and after the process of migrating their assets to the cloud. The purpose of this article is to conduct research and uncover the most effective security methods, as well as to discuss ways to enhance a security architecture in a corporate cloud environment. In addition to that, it will examine a few of the practice statements of cloud suppliers, as well as other cloud research literature, cloud reference architecture, and other cloud security frameworks. The use of cloud computing was discovered to be connected with a greater level of operational costs and a higher level of security risk. Therefore, the findings of this research will give some advice on the best security practices and architecture, which will enable organizations to make decisions that are better informed and to build designs that are more secure and can be implemented at a lower cost for their cloud environments.

Nedzelský, Roman (2015) Hybrid clouds, which include both private and public clouds, are a topic that is frequently brought up in contemporary day conversations. As a result of the fact that the majority of the data must be stored on hardware that is located on the premises and cannot be transferred to any public cloud, the hybrid solution is the only method for large corporations and state institutions to participate in the innovation that is taking place in cloud computing. Even if there are no legal restrictions inside the hybrid situations, businesses are concerned about the possibility of information leakage or other restraints that may occur when they do not have control over their data. On the other hand, it is quite tempting to take advantage of outplacement infrastructure, which the user does not need to worry about, or to utilize the services in the field of machine learning, business intelligence, stream analytics, and other SaaS features. Both of these options are very attractive. The migration to cloud solutions, or the utilization of cloud features, is a solution that is not only very desired but also extremely attractive from the perspective of cost savings. On the other hand, public cloud solutions are plagued by the fact that certain cloud services come with functions that cannot be utilized in conjunction with local servers that are located on the premises. A significant number of studies that have been conducted in recent times have concentrated only on the subject of private or public clouds. Within the context of hybrid clouds, this study focuses on the topic of security for major corporations and governments. It addresses the investigation of a variety of security types within the framework of the notion of infrastructure as a service (IaaS) and software as a service (SaaS), as well as a number of authentication and security principles, as well as

issues in terms of security in this field. The estimates supplied by Gartner, which anticipated that the majority of large enterprises will be adopting hybrid cloud scenarios in 2017, served as another source of motivation for this work which was carried out. In this study, a comparison is made between many different vendors who specialize in hybrid cloud solutions for government-related organizations. As a result of the fact that some of them are already offering cloud services with a concentration on the public sector, it is important to review these offerings and compare them with an emphasis on safety.

Donadio, Pasquale et al., (2014) The advent of cloud computing has made it possible to gain access to dispersed services in a transparent and elastic manner without having to invest in new infrastructures. Cloud computing has evolved from a potentially lucrative business idea to one of the most rapidly expanding sub-industries within the information technology sector over the course of the past several years. Enterprise clients are still hesitant to move their businesses to the cloud, despite all of the excitement that has surrounded the cloud. Security is one of the most significant challenges that inhibits the expansion of cloud computing, and complications with data privacy and data protection continue to plague the industry. Cloud computing is becoming increasingly popular. A Virtual Intrusion Detection System (V-IDS) is the emphasis of our proposed solution for the security of hybrid cloud environments, which is presented in this research. In order to protect cloud networks that are characterized by constantly changing underlying infrastructure and physical topology, we present a new architecture that takes into consideration the fundamental principles of cloud computing, virtualization, and the GMPLS Control Plane. This architecture then applies these principles to intrusion detection systems. We have validated our thesis by implementing a prototype of a cloud-based intrusion detection system (IDS) that is based on the architecture that we have outlined. Through the combination of two open-source technologies, namely OpenStack and DRAGON (Dynamic Resource Allocation over GMPLS Optical Networks), the prototype is brought into existence.

PROPOSED METHODOLOGY

For the purpose of tracing and preventing distributed denial of service (DDoS) assaults, as well as saving processing time, memory consumption, and bandwidth utilization, the suggested cloud security architecture has been devised and implemented. The paradigm that has been described is implemented in Centos 5, which is a variant of Linux that makes use of SQL Database and.NET. Through the utilization of VMWare, the virtualization environment was established by virtue of the creation of numerous workstations on a single node. This virtual machine is capable of connecting to the internet and running several instances at the same time. Using VMware, it is possible to allocate a distinct IP address to each individual computer. All requests are first routed through the request analyzer machine, which was installed and setup in front of the cloud network. After that, the requests are sent to the cloud network. A SQL database, the Centos 5 operating system, and a.NET framework are also installed on the request analyzer computer. These components allow the machine to retain logs and records of blacklisted hosts and to define rules. In order to determine how well the request analyzer performs its functions, we carried out a number of intrusion assaults on the system that was the target of the request while it was still in effect.

RESULTS AND DISCUSSION

During a DOS assault, the victim is subjected to an overwhelming amount of traffic, which in turn causes the system and network resources to be utilized. This includes the consumption of processing speed, the utilization of memory, and the decline in the availability of service. An intruder will send the identical requests over and over again within a short amount of time in order to make advantage of the network and system resources. This will cause the system to become so busy that it will be unable to respond to the user. The intrusion packet was transmitted to the server while it was contained within the requests wrapper. The purpose of the test was to analyze the system resources from the perspective of a single thread as well as numerous threads. In the first place, the assault was initiated in the form of a request from a single computer, and it was concluded that the amount of time, bandwidth, resources, and so on were all consumed. Following that, an assault is launched from numerous nodes, and it then proceeds to determine the bandwidth of the network and the resources of the system. In order to evaluate the performance of both the present model and the proposed model, the results that were generated based on the requests are displayed in Figure 1 and are also included in table 1.

Table 1 Comparison of Execution time

Data Size(KB)	Execution Time(ms)Existing Model	Execution Time(ms)Proposed Model
24	42	28
50	80	72
100	160	145
200	300	240
240	580	560

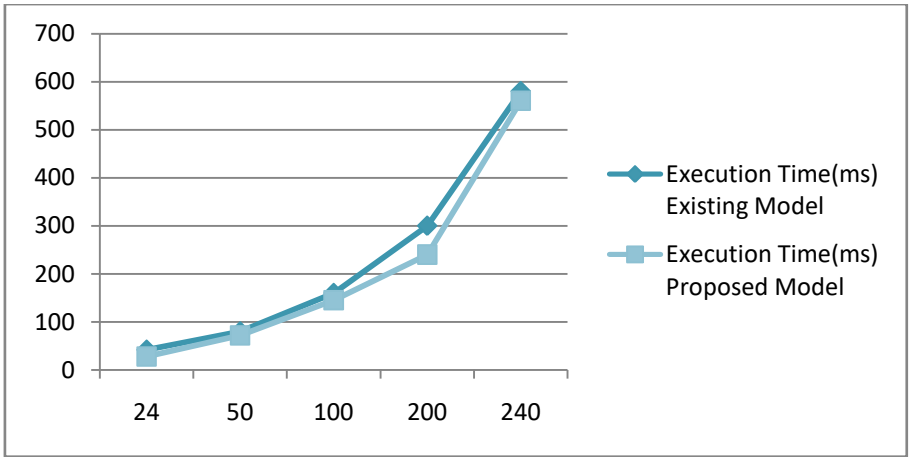

Figure 1: Comparison of Execution time

Compared to the findings that were presented, the execution time for the suggested model's filtration and prevention of requests is significantly faster. In addition, DDoS assaults were taken into consideration while calculating for multithread requests. The time required to execute the suggested model is less than that required by the present model. A model that has been proposed demonstrates that the execution time for single thread and multithread queries is quite short. In comparison to the model that is now in use, the suggested model not only decreases the amount of time required for execution, but it also improves the speed at which assaults are detected and prevented. The amount of bandwidth that an existing model consumes, as well as the amount of time that the CPU consumes, was also computed and tested. Because the suggested approach filters the new requests twice rather than once, it is able to minimize the amount of bandwidth that is actually used.

A request analyzer will block the requests for a certain amount of time if a distributed denial of service attack (DDoS) is being generated from the same sites within a short period of time. During a specified time period, it is unable to pass the specific and is unable to analyze the requests that are made from the same system. A secret code is provided to the host after a certain amount of time has passed in order to validate the request. This code is used to determine whether or not the request is being generated by a human being or an attacker who has penetrated the system and is automatically producing requests. Figure 2 and table 2 both display the results of the bandwidth calculation that was performed on both the existing model and the suggested model.

Table 2: Bandwidth Consumption in MB

Data Size in KB	Existing Model	Proposed Model
1000	03	02
10000	12	08
100000	90	70
1000000	510	250

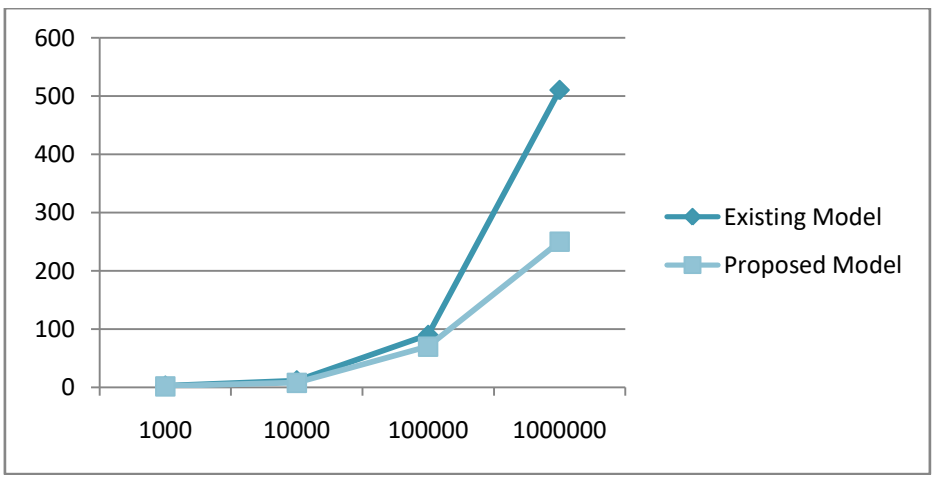

Figure 2: Comparison of Bandwidth Consumption in MB

Comparatively speaking, the proposed model has a lower bandwidth than the present model. The existing model is responsible for verifying and filtering each request that is received from the client, as well as producing an inspection report and an advice report. Two separate filters are applied to the request for each host in the model that has been proposed. In the event that the analyzer determines that the host is consistently creating requests containing incursion, then the request analyzer will block the host for a certain amount of time. After a certain amount of time has passed, a secret token is transmitted to a specific host in order to verify whether or not the request is coming from a human person or a hacked computer. Following the verification of the secret token by a specific host, the request analyzer determines whether or not the request contains any intrusions and then sends it to a cloud network. Amount of bandwidth In addition, the comparison ratio is displayed in the figure, which provides a clear indication of the performance of the suggested model.

CONCLUSION

The hybrid security method is effective because it can adjust to evolving threat scenarios and allocate resources in real-time by utilizing the flexibility and scalability of cloud infrastructure. Cloud settings can quickly and efficiently respond to new threats, reducing the impact of DoS and DDoS assaults on service availability and dependability. Protecting cloud settings from cyber attacks is crucial as cloud computing becomes more integral to current IT architecture. The hybrid security method provides a proactive and adaptable technique to reduce the risks of DoS and DDoS assaults, guaranteeing the integrity, availability, and dependability of cloud services for both companies and users.

REFERENCES

[1]. Mbah, Thierry. (2022). Architecture for Cyber Security Cloud Networks.
[2]. Garg, Deepak & Rani, Shalli&Herencsar, Norbert & Verma, Sahil & Wozniak, Marcin & Ijaz, Muhammad Fazal. (2022). Hybrid Technique for Cyber-Physical Security in Cloud-Based Smart Industries. Sensors. 22. 4630. 10.3390/s22124630.
[3]. Roy, Prince &Gujral, Rajneesh. (2021). A Hybrid Security Framework to Preserve Multilevel Security on Public Cloud Networks. 336-340. 10.1109/SMART52563.2021.9676271.
[4]. Anjali, &Velgeker, Sonu&Kamble, Nitin. (2021). A Study on Networking in Cloud Security. International Journal of Innovative Research in Computer and Communication Engineering. 9. 14493. 10.15680/IJIRCCE.2021.0911021.
[5]. Ferdous, Jannatul&Newaz, Fuad&Rezaul, Karim &Tamal, Maruf & Aziz, Md & Miah, Pabel. (2020). A Hybrid Framework for Security in Cloud Computing Based on Different Algorithms. International Journal of Network Security. 22.
[6]. Ebiriene, P.J. &Nwiabu, N.D.. (2019). An Improved Hybrid Cloud Computing Security Architecture Using Network Based Intrusion Prevention System. International Journal of Computer Sciences and Engineering. 7. 9-14. 10.26438/ijcse/v7i10.914.
[7]. Farnga, Max. (2018). Cloud Security Architecture and Implementation - A practical approach.
[8]. Bhardwaj, Akashdeep & Goundar, Sam. (2018). Algorithm for Secure Hybrid Cloud Design against DDoS attacks. International Journal of Information Technology and Web Engineering. 13. 10.4018/IJITWE.
[9]. Seth, Bijeta & Dalal, Surjeet. (2016). Designing hybrid security architecture in multi cloud system. 9. 317-325.
[10]. Nedzelský, Roman. (2015). Hybrid cloud computing: Security Aspects and Challenges.
[11]. Sharma, Avani& Goyal, Tarun& Pilli, Emmanuel & Mazumdar, Arka&Govil, M. & Joshi, R.. (2015). A Secure Hybrid Cloud Enabled architecture for Internet of Things. 274-279. 10.1109/WF-IoT.2015.7389065.
[12]. Nwafor, Ebelechukwu & Burge, L. (2015). A Hybrid Approach to Improving Cloud Data Security.
[13]. Donadio, Pasquale & Fioccola, Giovanni &Canonico, Roberto &Ventre, Giorgio. (2014). Network Security for Hybrid Cloud. 10.1109/EMTC.2014.6996640.
[14]. Yu, Wei & Xu, Guobin& Chen, Zhijiang&Moulema, Paul. (2013). A cloud computing based architecture for cyber security situation awareness. 2013 IEEE Conference on Communications and Network Security, CNS 2013. 488-492. 10.1109/CNS.2013.6682765.
[15]. Toubiana, Vincent &Labiod, Houda& Reynaud, Laurent &Gourhant, Yvon. (2010). A global security architecture for operated hybrid WLAN mesh networks. Computer Networks. 52. 218-230. 10.1016/j.comnet.2009.05.016.