iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** IV **Month of publication:** April 2018

DOI: http://doi.org/10.22214/ijraset.2018.4288

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue IV, April 2018- Available at www.ijraset.com

Cloud Unified Threat Management System

Prof. J. D. Jadhav[1], Vinita Ghotane[2], Rutuja Sapkal[3], Diksha Sawale[4], Priyanka Valiv[5]
[1, 2,3,4,5] *Department of computer engineering, Bharati Vidyapeeth's College of Engineering for Women, Dhankawadi, Pune, India.*

Abstract: Cloud computing is the future generation internet based computing system which provides easy and customizable services to the user to work with various cloud application. Many times the file which user are using gets corrupted through malicious attacks, which will harm to users system. So it's necessary to find that virus and remove it and protect users system. This paper will consist of information about user friendly web application for threat management based on Unified Threat Management System using middleware as AWS cloud. Functionalities of this UTM system will include pattern matching, signature verification, behavioural scanning, content filtering, vulnerability assessment a way of scanning and assessment for any extension of file with specified size & recovery of files. For user security, private account would be provided. To overcome the drawbacks of past UTM Systems which are hardware appliances, this project is built in cloud infrastructure so that it can be easily available for malware detection.
Keywords: AWS cloud, Security, Threat management, IDS, IPS.

I. INTRODUCTION

A. AWS help to create website

AWS can help you boost your online presence. Use AWS Elastic Beanstalk to create your own web app by selecting a name and platform for your environment. You can also host your website on AWS itself with the option of running it with or without a web server. AWS also allows you to name and register your own domain for your website. McCormick is just one example of how a company used AWS to expand their web presence. Using AWS, McCormock was able to support web traffic and launch their Flav or Print platform.

Unified threat management devices provide small or midsize businesses and heavily distributed enterprises with multiple network security functions in a single appliance. UTM buyers should evaluate performance, security, and ease of use, local support and UTMs' ability to handle new SMB practices. Unified threat management (UTM) is a converged platform of point security products, particularly suited to small and midsize businesses (SMBs). Typical feature sets fall into three main subsets, all within the UTM: firewall/intrusion prevention system (IPS)/virtual private network. Secure Web gateway security (URL filtering, Web antivirus [AV]) and messaging security (anti-spam, mail AV).

II. LITERATURE SURVEY

A. Title- High Speeed Classification Of Vulnerabilities In Cloud Computing Using Collabarative Network Security Management

Author- L. Krishnakumar, Nisha Mariam Varughese.

Year- 2013

Abstract- Security in open network is one of the major challenges with concerns such as Internet worms, Botnet, Phishing and Flooding attacks. To address the security problems collaborative network security management system is introduced with collaborative Unified Threat Management (UTM), traffic prober and cloud based security center. The security center can instruct each collaborative UTM and prober to collect raw traffic and this huge traffic is given to the data centre which classifies the data in parallel. Security centre will deeply analyse the classified data and generates new security rules. These security rules are carried out by collaborative UTM and the feedback events of such rules are given back to the security centre. The cloud storage is used to store the huge amount of internet traffic data and then processing it with cloud computing platform to detect the malicious attacks. Security centre analyse the data and when any attack is detected it will generate new rules. These rules are given to the network and feedback is evaluated. Then it will remove the invalid rules to make the system more efficient and reliable.

B. Title- Toward System Level Optimization For High Performance Unified Threat Management System.

Author- Yaxuan Qi, Baohua Yang, Bo Xu, Jun Li

Year- 2007

Abstract- To build holistic protection against complex and blended network threats, multiple security features need to be integrated into unified security architecture, which requires in a unified threat management (UTM). However, most existing UTMs operate by simply stringing together a number of security applications working independently without system level optimization that

streamlines processing flow and leverages shared information and resources to reach high performance. In this paper, a generic framework is proposed to optimize the performance of UTMs at both algorithmic and architectural aspects by exploring the idea of integrated protocol processing (IPP). The algorithm proposed in this paper improves overall protocol processing complexity of ACL and IDS from Theta (log (M) + log (N)) to Theta (log (M +N)). Experiments on Intel IXP2850 network processor show that our scheme outperforms existing solutions with 30% increase of throughput.

C. Title- Unified Threat Management System Approach For Securing Sme's Network Infrastructure

Author- Saqib Ali, Maitjam H. Al Lawati, Syed J. Naqvi

Year- 2012

Abstract- For many smaller and larger entities over the last couple of decades, information systems and technologies have become an integral part of their operations and played a major role in drastically changing and often improving their business processes. As computers become more and more integrated into our business organizations, we end up leaving and storing confidential, vital business and sensitive information on them. In general, larger organizations have the technical expertise and resources to better secure computing services. The Small to Medium Enterprises (SMEâs), however, often lack the platforms, infrastructure, technical expertise, and the required financial resources to be able to utilize modern secure technologies for computing services. This paper discussed the importance of network security, analyzed different type of threats to network infrastructure, different methodologies that can be used to mitigate network infrastructure threats and have proposed an approach for securing SMEâs network infrastructure. This approach suggested Unified Threat Management (UTM) as the first line of protection to the network, based on the links between each distribution switch layers which offers a zone based monitoring and controlling system to prevent the network from any possible threats.

III.SYSTEM ARCHITECTURE

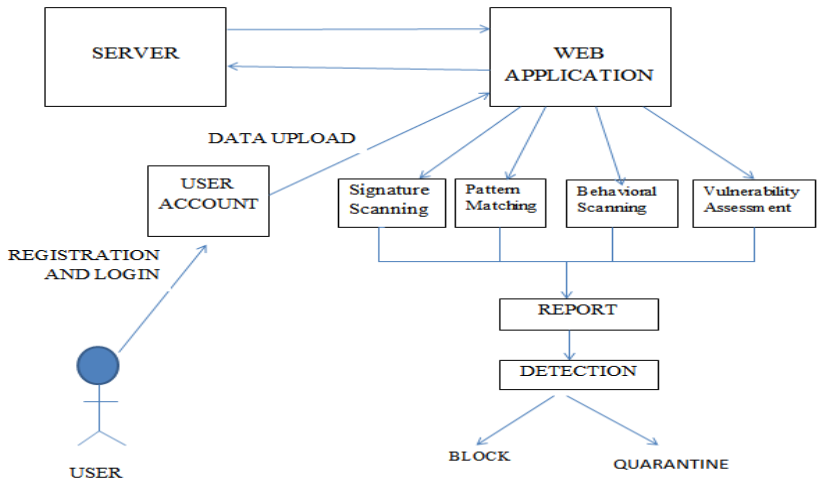


Fig. 1 System Architecture

The fig.1 shows the system architecture of this project, it also shown the components in the system like user, server, web application etc. Each component has a specific functionality in this system. This system is three tire architecture, as it is a web application. Where user works on the client side using the services provided by this application and the databases used for storing user data, signature databases and the network database together build up the data layer. AWS cloud is used as the interface between the client side and the data layer hence it is the server used in this application.

The client layer includes the front end developed in Visual Studio 2015 as an ASP .Net application using C# language. This front end is the interface between the user and application. It consists of login page, registration page, user dashboard and output dashboard. The tasks like user information entry, validating user, file upload or network range, and displaying result of the scan are assigned to the front end. The AWS serves as a server layer (middle ware) in this application. It is the interface between the client layer (front end) and the data layer (back end) it is done by establishing connection between front end (ASP .Net) and the back end (Mongo DB). AWS is a public cloud which supports and helps in rendering all the cloud services. And AWS is used as PAAS (Platform as a service) for developing business logic as well as deploying this web application. The data layer is the back end or the

storage layer in any system. Data stored can be in structured or unstructured form, in this application the data is stored in an unstructured format as to support distributed system. Mongo dB is used for storing user information, malicious code signatures, history etc.

The initial step for working with this application is creating a user account. A user can create his/her account by submitting the registration form available on the UI for user. The user account (i.e. their personal information) is secured and is uniquely identified by their Username and Password. Once the user has completed with his/her registration the next step is to login in their account. As the user has logged in their account they encounter various options on their dashboard like browse (for uploading a file) for scanning, two text areas for entering Public Network IP address and range for scanning the network for vulnerable data and its source IP. File scanning is a process where the uploaded file is first scanned and threat is detected if any. Also in network intrusion detection Anomaly Detection technique is used for detecting intrusion in the network and blocking the traffic through that IP. After the assessment of all scans the result is displayed on the output dashboard which includes all the assessment results of network or file. This result is also stored in the user's history with all the past records showing all the scans including network and file scan.

There is big process for file scan and they assessed on various parameters virus scan using 50 antivirus engines, malicious code detection using pattern matching. The following are the functions used for detection of threat in a file.

1) Antivirus engines: When you submit a file to antivirus for scanning it goes through a complex series of steps of fetching the files, scanning based on signature and/or heuristic and then further processing is based on the outcome.

The process for network scan for intrusion includes Network Behaviour Anomaly Detection, and Vulnerability Assessment. Following are the functions used for intrusion detection in a network.

2) Network Behaviour Anomaly Detection (NBAD): Including this type of detection UTM provides one approach to network security threat detection. NBAD is the technique where continuous monitoring of network for unusual events or trends is done. As this application uses NBAD thus this system is particularly helpful in detecting security threats vector in 2 instances. This program tracks critical network characteristics in real time and generates an alarm if a strange event is detected.

3) Vulnerability Assessment: It is an assessment for computers, computer systems, networks or applications for unknown weaknesses. Vulnerability Scanner is a computer program used for this assessment, these scanners are used to discover the weak points or poor constructed part. These are helpful for identification and detection of vulnerabilities relating to misconfigured assets or flawed software that resides on network-based assets such as firewall, router, web server, application server, etc.

The administrator has all the access rights to the database of user as well as the system databases. Admin has job to maintain, update and validate all the databases.

IV. MODULES

This system consists of three modules.

1) *Front End:* Front End is the interface between the user and the application, this system is a web application which consists of web forms and user dashboard. For Front End ASP .net. Front end consists of the login page, registration page, and user upload dashboard.

2) *Middle Ware:* Middle ware is the interface between front end and back end. AWS cloud is used to deploy the system as web application on a public cloud. Connectivity between front end and backend is established through the features of AWS cloud. For network security is achieved through security groups.

3) *Back End:* Back End is the storage unit where data is stored. As this system needs large storage, for large amount of storage non-relational database mongo DB is used.

V. FUNCTIONALITIES

The functionalities in this system include:

1) *Signature matching:* Signatures are the digital code representation of any file. It is a fixed code representing a file through hashing functions. Through pattern matching the signature scanning is done.

2) *Antivirus engine:* Antivirus engines are the engines which detect data for any virus. There are 51 engines included in this system.

3) *Behavioral scanning:* It helps to scan behavior of the packet in the network. It blocks the IP which causes the intrusion.

VI. CONCLUSIONS

UTM products originally were crafted based on the needs of smaller networks and smaller enterprises, and have seen broad acceptance in their large niche of potential installations. However, the concept of UTM has value in large networks and large enterprises as well. To support UTM in large networks, though, products must meet a very different set of requirements that set them apart from SMB-focused UTM firewalls. By going further in the areas of performance, network integration, support for consolidation, platform extensibility and flexibility, and management, UTM vendors can meet the needs of enterprise network managers. When UTM products reach to meet enterprise needs, the results are a powerful toolset that can displace traditional firewalls and give network managers greater flexibility and greater capability to solve their immediate security problems quickly.

VII. ACKNOWLEDGMENT

We would like to take this opportunity to express sincere thanks to the department and the University for this Course where we have such an opportunity to express our ideas and put our learning all the way into practice.

REFERENCES

[1] Saqib Ali, Maitjam H. Al Lawati, Syed J. Naqvi, "Unified Threat Management System Approach for Securing SME's Network Infrastructure",e-Business Engineering (ICEBE), 2012 IEEE Ninth International Conference on 9-11 Sept. 2012., **INSPEC:** 13372256, 10.1109/ICEBE.2012.36.

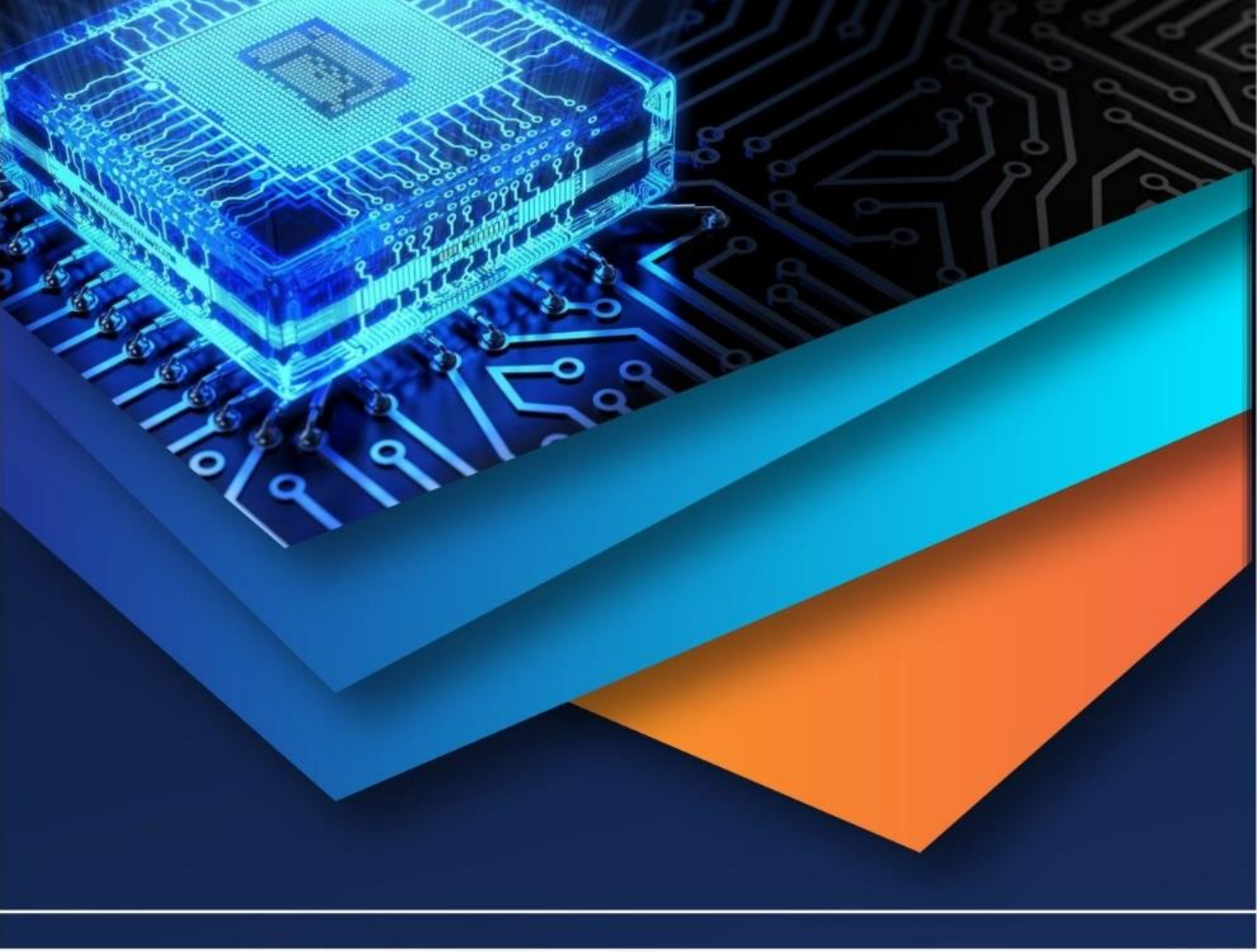
[2] Yaxuan Qi, Baohua Yang, Bo Xu, Jun Li, "Towards System-level Optimization for High Performance Unified Threat Management,"Networking and Services, 2007. ICNS. Third International Conference on 19-25 June 2007,**INSPEC:** 9812776, 10.1109/ICNS.2007.126.

[3] ZouheirTrabelsi, SafaaZeidan, Mohammad M. Masud, "Hybrid Mechanism towards Network Packet Early Acceptance and Rejection for Unified Threat Management,", " IET Information Security (Volume: 11, Issue: 2, 3 2017), 104 – 113.

[4] HuyAnh Nguyen, Deokjai Choi, "Network Anomaly Detection Flow based or Packet based approach", Anomaly detection, network monitoring, traffic measurement for network filtering. ISBN No.: 978-0-7695-3489-3, pp: 694-698.

[5] https://www.cyberoam.com/microsite/unified-threat-management

[6] https://en.wikipedia.org/wiki/Unified_threat_management



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY