Human Interaction and Emerging Technologies (IHIET-AI), Vol. 201, 2026, 619–627
https://doi.org/10.54941/ahfe1007215

Internet Bandwidth Allocation for University With Distributed and Centralized Protection Scheme

Senthilrajan Agniraj

Alagappa University, Karaikudi, Tamil Nadu, India

ABSTRACT

Networking the servers in the universities are developed with a standard configuration. Over the time, patches, updates, new software, versions, and mistakes or malicious activity, all lead to deviations across the university servers from this standard based. Malicious or unknown software, un managed switches in the networking can cause unexpected behaviour. To rectify these problems well managed enterprises plan for quality of protecting the servers and nodes as well as sharing the bandwidth of internet connectivity throughout the university campus is needed. This involves eliminating and implementation of certain actions in the main server and university campus networking. The level of protection is dependent upon the day of usage of internet band width in the university campus. Certain rules, security and assurance in the campus networking will be exercised based upon the cyber environment. This may exercise in different ways when communication is needed across various departments and buildings in the university campus. To minimize and to protect the server and nodes from viruses, scanner and disabling of devices or interfaces a proposed method will be implemented. The proposed method also involves identifying and fixing issues in the university campus networking. This requires a central rule for the server and university campus networking to quickly identify potential issues and a method of remotely taking action to either fix the affected system or freeze it until further actions can be taken. This paper discusses the current approach to centralize the monitoring of communications in distributed approach and relies on a well-formed security in the university campus.

Keywords: Servers, Traffic, Inspections, Protections, IT, Security, Encryption key

INTRODUCTION

Alagappa University has emerged from the galaxy of institutions initially founded during 1950's by the Padma Bhushan Dr. RM. Alagappa Chettiar (06.04.1909 - 05.04.1957). Alagappa University is a State Government University established by an Act of the Tamil Nadu State Legislature in 1985 as Unitary type; later became Affiliating type during 2002. The University is situated at Karaikudi, in the District of Sivaganga, in the State of Tamil Nadu. Alagappa University's campus sprawls across 435.98 Acres of lush land, (428.15 acres in Main Campus and 7.83 acres in Thondi Campus) creating a highly secure, eco conscious and student friendly learning ambience.

Received November 5, 2025; Revised November 28, 2025; Accepted December 13, 2025; Available online April 1, 2026

Network

In Alagappa University there are several buildings, out of which 64 are used for academic and administrative use.60 buildings have world class Internet, Wi-Fi and CCTV, facilities. Zero Trust Infrastructure. Zero Down time. Planned for ISO 27001-22 Standardized and structured architecture. Scalability for another 10 years. Secured Infrastructure.

Structure

The Core domain for the internet is a Server room where the internet will distribute to each department buildings and administrative building. The internet also distributed to the computer labs. Class rooms and staff rooms. There is a mechanism to segregated all collusion domain and also VLANs divide a physical network into multiple logical networks. The university has different types of internet service provider and they are BSNL 100 MBPS 1:1 LEASE LINE where optical input received from Bharat Sanchar Nigam Limited along with 32 numbers of public internet protocol. The second connection is National knowledge network

1GBPS leased line with 16 public internet protocol. Every building in the university campus is well connected by optical fiber and the planning the route by Considering certain parameters such as Location of Building, Septic Tank, Electrical, Plumbing line route etc.

Protection

University computer systems protection is based upon the device, the environment, and the types of users. Alagappa university have a powerful Sonic firewall which protects the entire campus internet security. Enclave is a collection of entities and assurance mechanism that uniformly employed the same security. Security Prediction includes on device using the MAC id authentication , software, in-line, monitoring of communications, and in particularly security model that provides confidentiality, integrity and the availability. All WIFI users are freely accessing the internet inside the university campus by providing the password protection system. Many times, the security model is compromise in trying to provide basic levels of protection. This compromise may include policy base instructions to configure and give direction to the devices which provides the capability for selecting heavy attacks or monitor. These policies selections can be providing capabilities to select what responses will be taken for each direct intrusion.

CURRENT PROTECTION APPROACHES

Elements involved in implementing quality of protection are numerous and complicated. Wide ranges of servers are used to provide functionality ranging from quality of service to the user or quality of protection of network resources and service (Oppliger, 1997). These applications are often placed in line and some required across to the content.

The number of servers can be quite high. Below is a parallel list of functional types.

1. Header based scanner /logger
2. view only and encrypted, potion of traffic
3. Synchronous or asynchronous operation
4. Scans for suspicious behavior logs, traffic.
5. Content based scanner logger
6. Views, content, sickness or a synchronous operation stands for suspicious behavior, logs, traffic and content
7. Header based firewall, use only an incompetent, question of traffic, synchronous, operation, stands for blogs, suspicious behavior
8. Content based firewall blocks only the View decrypted content, synchronous operation, scan for suspicious behavior and blocks connections.
9. Load balancer which distributes load among destination end points to improve through put and reduce latency.

CURRENT UNSCRIPTED TRAFFIC

To understand the current paradigm, a review of what is done through a portal for an encrypted traffic is provided. HTTP traffic is an encrypted from browser to portal, and unencrypted from portal to web applications, providing content, examples are man in the middle model for applications, and another example are firewalls, deep packed inspection and accelerator. Portal is the end point for the browser requests (K. Selçuk Candan, 2001). Load balancers and some firewalls may be treated a passive entity in this treatment.

Current Encrypted Traffic

When traffic is encrypted; the same basic approach is adapted to handling traffic inspection. HTTPS traffic is successfully decrypted and re-encrypted when it is needed (Conway, 2004). End to end HTTP traffic is encrypted using transport layer, security from browser to portal and using separate TLS (Transport Layer Security) sessions from portal to web applications (Senthilrajan.A, 2019). Some can function without decryption, example is firewall, some required decryption, using portal, privately, example is deep packet, Inspection and accelerator Portal is the endpoint for the browser request.

PROPOSED METHODOLOGY

In order to prevent attackers from gaining access to networks, each device must monitor DHCP requests and report to the central monitor all such requests. This provides listeners throughout the network that allow the central monitor to quickly identify the requesting entity, determine whether it is a known and trusted device or a rogue entity, and take action accordingly. Any system that is found on the network, through DHCP or other traffic, must identify itself to the protection system before any services are provided to it (William R. Simpson, 2008). This identification

is through protection system communications, through which each device authenticates to the central authority and also authenticates the central authority. All such traffic uses end-to-end security, and all devices and their protection systems are registered with enterprise. Unknown entities are not given services and are marked as rogue, which enables local devices to ignore their traffic. Allocation of bandwidth to the university department as well as to users are done by the system administrator (T. O. Paulussen, 2023). The system administrator allocates the internet bandwidth using the internet protocol (I.Vermeulen, 2006) with the help of TACITINE hotspot (see Figure 1 , Figure 2).

Figure 1: TACITINE HS5200 HOTSPOT – TOTAL USAGE DATA SIZE (Details such as Date, Total bytes downloaded, Total bytes uploaded are displayed).

Date	Source IP	Source MA	Protocol	Port	Service	Total Byte	Connectic	Dest IP	Downloac	Upload	By User	Host Name
Oct 17 202	10.0.22.11	D8:F8:83:E	tcp	443	HTTPS	4042	1	35.190.80.	1684	2358	-	DESKTOP-MVQD8BB
Oct 17 202	172.23.13.	3c:2c:30:e	tcp	443	HTTPS	9896	1	142.250.1(	6355	3541	muthukur	-
Oct 17 202	172.23.14.	-	tcp	443	HTTPS	6015	3	23.100.10(	4629	1386	-	-
Oct 17 202	10.0.34.51	84:FD:D1:(	udp	443	QUIC	7668	1	35.186.25(	0	7668	gowthami	ADMIN
Oct 17 202	172.23.7.7	3c:ec:ef:9	tcp	443	HTTPS	10429	2	34.107.24(	3713	6716	r20162719	-
Oct 17 202	172.23.14.	a0:8c:fd:cl	tcp	443	HTTPS	8867	1	23.48.245.	7935	932	rashiya	-
Oct 17 202	172.23.30.	10:62:e5:0	tcp	443	HTTPS	24469	2	142.251.4(	7842	16627	sk_pandia	-
Oct 17 202	172.23.32.	3c:ec:ef:a	udp	443	QUIC	7668	1	142.250.7(	0	7668	kbalamur	-
Oct 17 202	172.23.20.	2c:58:b9:1	tcp	443	HTTPS	9326	1	172.217.2(	4702	4624	rajasekarc	-
Oct 17 202	172.23.8.7	c4:65:16:0	tcp	443	HTTPS	19225	2	35.244.25(	4334	14891	phdnacha	-
Oct 17 202	172.23.13.	3c:2c:30:e	tcp	443	HTTPS	7265	1	18.161.21(	6048	1217	muthukur	-
Oct 17 202	172.17.17(	6c:92:cf:0(	tcp	443	HTTPS	13698	1	142.251.2(	5361	8337	-	-
Oct 17 202	172.23.7.1	2c:58:b9:e	tcp	443	HTTPS	2634	1	20.42.65.8	2017	617	-	-
Oct 17 202	172.23.11.	-	tcp	443	HTTPS	7683	1	172.202.6(	6182	1501	r20223132	-
Oct 17 202	172.17.6.5	a0:8c:fd:cl	tcp	443	HTTPS	150859	2	23.202.22(	142248	8611	-	-
Oct 17 202	172.17.17(	6c:92:cf:0(	tcp	443	HTTPS	9869	1	150.171.4(	8490	1379	-	-
Oct 17 202	10.0.48.21	44:46:87:4	tcp	443	HTTPS	4195	1	142.251.2(	1884	2311	-	realme-5s
Oct 17 202	172.16.7.1	c8:d3:ff:3(	tcp	443	HTTPS	11282	1	142.251.2(	7123	4159	haribaskai	-
Oct 17 202	172.18.10.	-	tcp	443	HTTPS	42771	2	150.171.2(	23857	18914	dharumar	-
Oct 17 202	172.23.7.1	2c:58:b9:e	tcp	443	HTTPS	7203	3	20.42.73.3	5055	2148	-	-
Oct 17 202	172.23.10.	e0:73:e7:1	tcp	443	HTTPS	34463	5	18.246.92.	26830	7633	wilson	-
Oct 17 202	172.23.10.	e0:73:e7:1	tcp	443	HTTPS	10915	1	142.250.2(	8711	2204	wilson	-
Oct 17 202	172.23.4.5	-	tcp	443	HTTPS	35050	1	23.44.10.1	27585	7465	Srini	-
Oct 17 202	10.0.46.59	3C:91:80:6	tcp	443	HTTPS	32510	1	142.250.7(	28498	4012	2.02E+09	DESKTOP-7JNA6E3
Oct 17 202	10.0.41.19	28:C5:D2:E	tcp	443	HTTPS	14561	2	3.164.85.1	8728	5833	phdarunm	Arun
Oct 17 202	172.23.7.1	ac:1f:6b:8	tcp	443	HTTPS	8091	1	142.251.2(	4114	3977	phdr2016	-
Oct 17 202	10.0.46.14	40:23:43:0	tcp	7680	-	3590	6	172.17.6.5	1560	2030	saruit	DCL-LAB9
Oct 17 202	172.23.13.	3c:2c:30:e	tcp	443	HTTPS	53760	1	20.49.150.	9170	44590	muthukur	-
Oct 17 202	172.17.50.	7c:57:58:3	tcp	443	HTTPS	10913	1	172.217.2(	4810	6103	-	-
Oct 17 202	172.16.7.1	c8:d3:ff:3(	tcp	80	HTTP	1444	2	117.239.2(	798	646	haribaskai	-
Oct 17 202	172.23.14.	04:95:e6:a	tcp	443	HTTPS	49604	1	52.71.166.	37499	12105	phdr2016	-
Oct 17 202	172.16.18.	14:cb:19:6	udp	443	QUIC	7668	1	150.171.2(	0	7668	krithikac	-
Oct 17 202	10.0.10.10	E8:51:9E:2	tcp	443	HTTPS	29598	10	20.106.10(	19716	9882	-	WA65C
Oct 17 202	10.0.34.23	3C:91:80:6	tcp	443	HTTPS	18258	2	172.217.2(	7875	10383	phdr2022	DESKTOP-2507VVV
Oct 17 202	172.25.2.6	-	tcp	443	HTTPS	7629	1	142.250.7(	4638	2991	-	-
Oct 17 202	10.0.51.80	00:45:E2:1	tcp	443	HTTPS	23583	2	142.251.2(	11808	11775	phdr2016	DESKTOP-AA59L8P
Oct 17 202	172.23.11.	-	tcp	443	HTTPS	10501	1	18.161.22(	8155	2346	r20223132	-
Oct 17 202	172.24.4.6	a0:8c:fd:cl	tcp	80	HTTP	6755	3	18.139.25(	2802	3953	alaguganc	-
Oct 17 202	10.0.56.85	0C:96:E6:9	tcp	443	HTTPS	3999	1	142.251.2(	1764	2235	-	DESKTOP-PCO4DE7
Oct 17 202	10.0.52.9	9E:95:01:9	tcp	443	HTTPS	18059	2	57.144.21(	7670	10389	manikand	V2225

Figure 2: Data shows the numbers of users, IP Address, connections and Bytes used.

IMPLEMENTATION ARCHITECTURE

The university network would have multiple layers to support this hybrid model.

1. Centralized protection: Located at the heart of the network, this is where the main internet connection resides. A border firewall and IPS protect the entire campus from external threats.
2. Hybrid protection: This layer connects the core to the access layer. Multiple firewalls can be used here to separate administrative systems from academic and residential areas, each with its own security policy.
3. Distributed protection: The access layer connects end-user devices in dorms, classrooms, and offices. Local security measures, such as network access control (NAC) and endpoint security, are enforced at this level. A Wi-Fi security framework using RADIUS authentication would secure wireless access.

Key security measures

- Network segmentation can be implemented in the university campus where network is divided into smaller, isolated segments. This prevents threats from spreading laterally across the network and protects sensitive information. Identity and access management using this technology all network users are authenticated and given role-based permissions to control access to specific resources.
- Threat monitoring and detection: An Intrusion Detection System (IDS) continuously monitors traffic for malicious activity and alerts the IT team of potential threats.
- Secure remote access: A Virtual Private Network (VPN) provides a secure, encrypted tunnel for off-campus users to access university resources.
- Security awareness training: Regular training for students and staff on best practices helps mitigate risks from human error.

EXPERIMENT

Experiment was carried out from the R statistical programming. Surveys are effective at collecting data by analysis of variance (ANOVA) or ANOVA testing. In the field of statistics, the Analysis of Variance (ANOVA) is a powerful and widely used technique for comparing means across multiple groups. ANOVA test provides researchers and data analysts with valuable insights into the variations between different groups and the effects of various factors.

Analysis of Variance (ANOVA) is a powerful statistical technique used to compare the means of two or more groups. It is widely employed in various fields, including psychology, biology, economics, and engineering, to name a few. It helps researchers understand whether there are statistically significant differences among the group means and if those differences are due to random chance or actual effects. ANOVA is particularly useful when dealing with categorical data or when comparing the effects of different treatments

or interventions on a continuous outcome variable. The basic idea behind ANOVA is to decompose the total variance in the data into two components: variance between groups and variance within groups. If the variance between groups is significantly larger than the variance within groups, it suggests that there are genuine differences between the groups being compared. Two types of ANOVA are used for the experimental purpose and they are One-way ANOVA and Two-way ANOVA.

Source Code

```
install.packages(c("ggplot2","ggpubr","tidyverse","broom","AICcmodavg"))
library(ggplot2), library(ggpubr), library(tidyverse), library(broom), library(AICcmodavg)
#ONE WAY ANNOVA
z<-read.csv("report.csv")
one.way<-  aov(z$Port ~ z$Connections)
one.way
summary(one.way)

#To check whether the model fits the assumption of homogeneity,
par(mfrow=c(1, 1))
plot(one.way)
z<-read.csv("report.csv")

#TWO WAY ANNOVA
two.way<- aov(z$Port ~ z$Connections + z$Total.Bytes)
summary(two.way)
par(mfrow=c(1, 1))
plot(two.way)
```

Interpretation of the Results

```
summary(two.way)
              Df    Sum Sq  Mean Sq F value   Pr(>F)
z$Connections      1 3.191e+07 31908268  14.457 0.000144 ***
z$Total.Bytes      1 6.295e+05   629495   0.285 0.593312
Residuals      99997 2.207e+11  2207177
---
Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1
```

Here is a breakdown of what each column means:

- Df: Stands for "Degrees of freedom." This is the number of independent values that can vary in an analysis. For the z$Connections factor, Df = 1, indicating that there were two groups or levels being compared.
- Sum Sq: Stands for "Sum of Squares." This value measures the variation within your data that is explained by the Connections factor. In this case, it is 3.191e+07, or 31, 908, 268.
- Mean Sq: Stands for "Mean Square." It is calculated by dividing the Sum of Squares by its corresponding Degrees of Freedom ($MS = SS / Df$). This

is a variance estimate.For z$Connections, the mean square is 31, 908, 268/1=31, 908, 268.

- F value: This is the F-statistic, a test statistic used to determine if the variation between the groups is significantly larger than the variation within the groups. It is the ratio of the Mean Square of the factor (z$Connections) to the Mean Square of the residuals (*F = MSConnections / MSResiduals*). The calculated F-value is 14.46.
- Pr(>F): This is the p-value, which represents the probability of observing an F-statistic as extreme as 14.46, assuming the null hypothesis is true (i.e., assuming there is no difference between the groups). The p-value is 0.000144.
- Signif. codes ():* These codes provide a quick visual indicator of the p-value's significance. The *** indicates that the p-value is very small (p<0.001, p is less than 0.001), meaning the result is highly statistically significant.

The results indicate that the z$Connections factor has a highly statistically significant effect on the response variable. The large F value (14.46) suggests that the variation between the groups defined by Connections is much larger than the unexplained random variation. The very small p-value (0.000144), confirmed by the ***, leads to the rejection of the null hypothesis. This means that the differences between the group means of the Connections variable are unlikely to be due to random chance. The top row shows the interpretation of two-way ANOVA and the bottom row shows the interpretation of one-way ANOVA with parameters of Residuals versus Leverage, scale location, Residuals versus Fitted (see Figure 3).

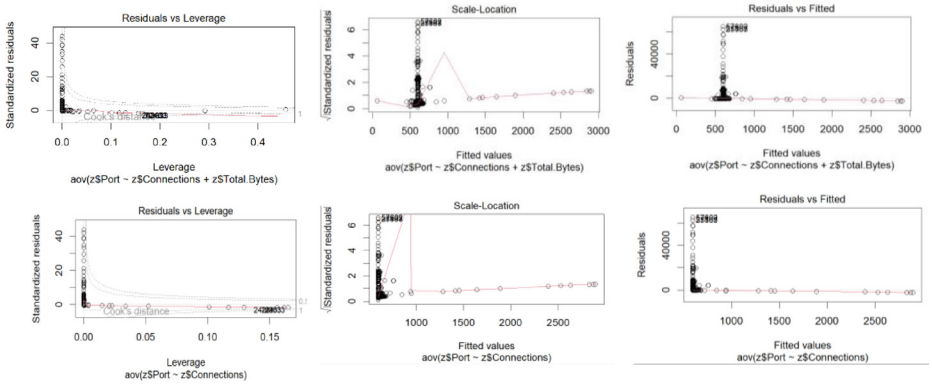

Figure 3: Two- Way ANOVA and One-Way ANOVA.

CONCLUSION

The distribution of private keys is a fundamental violation of a high assurance model. Effective Internet bandwidth allocation is crucial for ensuring optimal network performance, security, and user satisfaction within a university environment. A centralized protection scheme offers strong control, simplified

management, and consistent security enforcement across all departments, making it suitable for institutions requiring strict policy compliance and easier monitoring. On the other hand, a distributed protection scheme provides flexibility, scalability, and localized control, allowing individual departments to manage their own resources efficiently while reducing bottlenecks in the central system. An optimal approach may involve a hybrid model that combines centralized oversight with distributed control, ensuring both high performance and strong security. By carefully planning bandwidth allocation policies, implementing intelligent traffic management tools, and adopting layered protection mechanisms and AI based techniques may be implemented so that university can achieve balanced resource utilization, improved service quality, and a secure digital learning environment.

REFERENCES

Cain, B., Spats check, O., May, M., and Barbir, A. (2001). Request routing requirements for content internetworking. http://www.ietf.org/internet-drafts/draft-cain-request-routing-req03.txt.

Carlos Cunha, Azer Bestavros, Mark Crovella (1995). Characteristics of WWW Client-based Traces. Boston University, Boston, MA.

Chang, Rocky (2002). Defending Against Flooding-Based Distributed Denial-of-Service Attacks: A Tutorial. IEEE Communications Magazine 40 (10): 42–43.

Conway, Richard, Code Hacking (2004). A Developer's Guide to Network Security. Hingham, Massachusetts: Charles River Media. p. 281. ISBN 1-58450-314-9.

Erich Gamma, Richard Helm, Ralph Johnson ed. (1995). Design patterns: elements of reusable object-oriented software, Addison-Wesley Longman Publishing Co., Inc., Boston, MA.

I.Vermeulen, s.Bohte, K.Somefun (2006). İmproving patient activity schedules by multi-agent Pareto appointment exchanging. Proc. of the 8 th IEEE Conference on E-Commerce Technology (CEC 06).

K. Selçuk Candan, Wen-Syan Li, Qiong Luo, ed. (2001). Enabling dynamic content caching for data base driven web sites, Proceedings of the 2001 ACM SIGMOD international conference on Management of data, pp. 532–543, May 21– 24, 2001, Santa Barbara, California, USA [doi>10.1145/375663.375736]

Oppliger, Rolf (May 1997). Internet Security: FIREWALLS and BEYOND. Communications of the ACM 40 (5): 94.

Senthilrajan.A (2019). A Heuristic Fuzzy Algorithm for Hardware Engineers Assignment in University Sectors. Human Interaction and Emerging Technologies Proceedings of the 1st International Conference on Human Interaction and Emerging Technologies (IHIET 2019), DOI: 10.1007/978-3-030-25629-6_35, August 22–24, 2019, Nice, France.

T.O.Paulussen, N.R.Jennings, K.S.Decker, A.Henzl (2003). Distributed patient scheduling in hospitals. Proc. of the 18 th International Joint conference on Artificial Intelligence, pp. 1224–1229.

Virgílio Almeida, Azer Bestavros, Mark Crovella, ed (1996). Characterizing reference locality in the WWW, Proceedings of the fourth international conference on Parallel and distributed information systems, pp. 92–107, Miami Beach, Florida, USA.

William R. Cheswick, Steven M. Bellovin, Aviel D. Rubin (2003). Google Books Link. Firewalls and Internet Security: repelling the wily hacker.

William R. Simpson, Coimbatore Chandersekaran and Andrew Trice (2008). A Persona-Based Framework for Flexible Delegation and Least Privilege. Electronic Digest of the 2008 System and Software Technology Conference, Las Vegas, Nevada.

William R. Simpson, Coimbatore Chandersekaran and Andrew Trice (2008). Cross-Domain Solutions in an Era of Information Sharing. The 1st International Multi-Conference on Engineering and Technological Innovation: IMET2008, Volume I, pp. 313–318, Orlando, FL.