BYOD Secured Solution Framework

Md Iman Ali, Sukhkiran Deep Kaur

Abstract—This research focuses on Secured design architecture of BYOD solution. Bring your Own Device is a project driven in most of the enterprises to provide internet access to employee personal devices and Guest users. It has resulted in a trend to give Access to Employees Smart phones, tablets and personal to improve employee productivity and address changing working preferences in todays digital age. The Enterprises areBenefiting by providing lesser Devices to their Employees, this is one of the major reasons for the Enterprise to invest in BYOD Infrastructure. Slowly BYOD becomes a rule rather exception. The BYOD Infrastructure provides their Employees an access to the Internet while being a trusted user accessing the Enterprise infrastructure, which is intended to be Secure. The BYOD Infrastructure also provides Employees to grant Guest User Internet Access to their Visiting Partners as well. Connecting external devices in Corporate network increases the cyber security risk and data leakage incident. Using BYOD services users can do malicious activities, try to gain unauthorized access to internal network which can lead into major security breach. Providing Internet access to the external devices using internal corporate network has resulted in a challenge in addressing significant Security risk, data theft and Shadow IT because of unsecured design architecture that compromise the security policy. Installing malware in BYOD and connecting to Internet network can also lead into serious damage and major security risk. A major concern is also to revoke internet access while employee is no more in the system. Incase if employee left and access does not get revoked on time also can be a risk. Poor BYOD design significantly lead into organization Cyber security risk. The Research Paper has Demonstrated the Use Case for Trusted User access and Untrusted Guest User access and Monitoring of the BYOD—User activity and Audit compliance. In this research paper, a secured Design Architecture, Implementation and analysis is conducted. A practical analysis is conducted regarding the design and a Secure BYOD model is demonstrated. This study also highlights the Secured model of BYOD implementation maintaining organization laid down security policy so that enterprise CEO, CIO, CISO can address concerns for securing the Enterprises BYOD Infrastructure.

Keywords—BYOD, Security, BYOD framework

I. INTRODUCTION

With the growing rate of Internet access required in working environment on employee’s personal devices, the phenomena called as BYOD. Bring your own device in the organization and providing internet access to personal devices become primary requirement for the organization IT department. BYOD becomes rule rather exception over the time. BYOD solution which is used in almost all the organizations, universities, institutions. BYOD provide the internet access to personal devices like mobile, tablet and other internet devices. Bring your own device in the organization provide the extra luxury facility for employee satisfaction and need to seamless internet access within the organization boundary.

BYOD services involved very high security risk and threats to the organization. Allowing internet access to employees personal devices can lead into potential security risk, data leakage, loss of control if proper security mechanism is not in place[1]. Using mobile devices for personal and professional work itself has security risk[2]. Specially design architecture of BYOD is very critical in nature, ignorance on BYOD design can lead into a major security and organizational potential data loss. Then how the BYOD should be design? in an organization there can be 2 different set of BYOD users like employee which an active directory user and guest wifi access to the users who are not active directory users, untrusted users. How this 2 types of users can be segregated and create secure solution of BYOD? This study purely focus on the design architecture and analysis of the security parameter and how to create two different security architecture using the same wireless architecture. Finally after test and analysis this study suggest a framework of creating a secure model of BYOD architecture for corporate wireless, Employee personal devices access and Guest user access.

This study also analyse a new and highlight the security risk of using traditional BYOD services to the cloud data which is organization private cloud data which is new study area.

But data protection mechanism is also crucial part while giving internet access to the personal devices using same Wireless Access point and wireless controller. While implementing BYOD solution organization need to maximize the advantage but minimize the risk[3]. Organization need to be aware of security risk while designing and implementing the BYOD solutions. Since same Wireless access point need to be used in corporate wireless services and BYOD wireless service. Employee satisfaction of an organization is measured with quality of work culture and facility to the employee. As internet becomes one of the fundamental component of for the employee, now a days. Every employee of an organization has minimum of 2/3 devices at all the time. Official and personal. BYOD market About to hit $367 billion by 2022, up from just $30 billion in 2014 (Source: BetaNews). While in official Laptop employee gets internet services and security policies are defined in the perimeter firewall and all the web gateways. But every employee demands internet services on their personal devices.

Giving Internet access in personal device using the same wireless Access Point and the controller traffic segregation normally done with SSID, layer 3 authentication etc. While giving internet access to their personal devices as the concept called as “Bring your own device”. BYOD design has certain limitations.

II. DESIGN METHODOLOGY FRAMEWORK

Proposed BYOD Secured model for Employee own personal device and Guest personal devices are both segregated design. Design and access method of three different segment of architecture using same wireless access point and wireless controller along with AAA server and user database.
BYOD Secured Solution Framework

are shown in 3 different figure.

2.A CASE-1: BYOD-Trusted-User: AD user

In this scenario BYOD user is the user who is an employee of the organization and user id is retrieved from active directory domain controller. User authentication mechanism is based on the existence of the user id in Active directory employee database. Block diagram Architecture for BYOD-Trusted-Employee devices having userbase in organization active directory.

2.B TESTING COMPONENTS USED FOR THE DEMONSTRATION

Testing has been done with below components products with their make and model.

| Seq# | Technology/Service                  | Product used for test       |
|------|-------------------------------------|-----------------------------|
| 1    | AAA server                          | Cisco Identity Service Engine |
| 2    | Internal Firewall                  | Cisco Firewall              |
| 3    | External Firewall                  | Checkpoint Firewall         |
| 4    | Anchor Controller                   | Cisco WLC 5508              |
| 5    | Mobility Agent                      | Cisco 3850                   |
| 6    | Active directory                    | Microsoft AD                |
| 7    | Router                              | Cisco Router                |
| 8    | BYOD devices                        | Android/Iphone              |
| 9    | Corporate Device                   | Laptop                      |

Table-1: Products/devices used during the test.

2.C Traffic flow for BYOD architecture during the test

Traffic flow of the BYOD-Trusted-User having user entry in Active Directory

| Seq# | Source            | Destination       | TCT/UDP Port |
|------|-------------------|-------------------|--------------|
| 1    | Foreign Controller| AAA server        | 1812         |
| 2    | BYOD user         | DNS               | 53           |
| 3    | BYOD user         | AAA server        | 8443         |
| 4    | BYOD user         | AAA server        | 8905         |

Table-2: Traffic flow with port numbers

1st packet of the BYOD device is towards AAA server on port 1812 as authentication request but this is proxied through Foreign controller, post user gets Pre-auth IP address from External Firewall

As shown in Fig-1 BYOD device directly land up in External Firewall segment bypassing the corporate network.

This user traffic is not seen anywhere in the corporate network even though same access point is used.

Security risk[4] and policy compliance of the organization and protection of core infrastructure from BYOD device is maintained with this approach. Implementing BYOD crashes will Security breach[5] and will be bigger impact to organization data.

While BYOD device will connect the SSID “BYOD-Employee” will get pre-auth IP which does not have any access apart from reachability of the AAA server and DNS.

2nd Packet will goto DNS for resolution of the Certificate name.

In this study authentication method is PKI used as Certificate based authentication which is most secured and encrypted[6] method of authentication of 802.1x. Purely layer 2 model of authentication has been used. In this test this is configured and tested until certificate based authentication happened user will not get the Post auth IP.

2.C.1 TRAFFIC FLOW CHART

Flow of authentication as mentioned below

As shown in fig-2 when BYOD user request for authentication with a proxy of wireless Lan controller, request goes to AAA server (1) and then AAA server request to User data base (2) back to back to authenticate valid user and active user. Post AD respond back to AAA with response as “Valid”, it redirects for certificate and here the main point for 802.1x authentication mechanism to be used which is secured[7] model. In this phase BYOD
device gets the certificate (5). Then AAA server response back to Anchor controller to change the VLAN, which is called Post auth VLAN (Internet access IP).

Post-auth Network segment will have access of Internet. This policy is on external firewall only as below

| Seq | Source | Destination | Port | Natting |
|-----|--------|-------------|------|----------|
| I   | Post Auth VLAN | Any | Any | Yes |

Table-1: Firewall policy for internet access

In this stage BYOD-Trusted Employee will get internet access without any IP routing of this Network in corporate internal network. The major security concern of connecting personal device[8] in corporate network is addressed in segregating the BYOD Segment and with certificate based secured authentication. In this case security posture[9] and associated risk are also addressed because vulnerable device can be major security threats. BYOD design should comply security policies of the enterprise[10]. In this test this is completely segregated from corporate network.

III. RESULT AND ANALYSIS

Test result and analysis of the BYOD-Trusted-Users with EAP-TLS secured certificate based authentication.

Steps during authentication, logs from AAA server, this test is done with the BYOD device MAC address: 94:65:2D:E8:A4:89

| Event #  | Event Details                                                                 |
|----------|-----------------------------------------------------------------------------|
| 11001    | Received RADIUS Access-Request                                              |
| 11017    | RADIUS created a new session                                                |
| 15049    | Evaluating Policy Group                                                     |
| 15008    | Evaluating Service Selection Policy                                         |
| 11107    | Extracted EAP-Response/Identity                                             |
| 12300    | Prepared EAP-Request proposing EAP-TLS with challenges and configured       |
| 12625    | Valid EAP-Key-Name attribute received                                       |
| 11006    | Returned RADIUS Access-Challenge                                            |
| 11001    | Received RADIUS Access-Request                                              |
| 11018    | RADIUS is re-using an existing session                                      |
| 12502    | Extracted EAP-Response containing EAP-TLS challen                           |
| 12800    | Extracted first TLS record; TLS handshake started                           |
| 12305    | Extracted TLS ClientHello message                                           |
| 12806    | Prepared TLS ServerHello message                                            |
| 12807    | Pre-processed TLS Certificate message                                      |
| 12808    | Pre-processed TLS ServerKeyExchange message                                |
| 12809    | Pre-processed TLS CertificateRequest message                               |
| 12805    | Pre-processed EAP-Request containing another EAP-TLS challenge              |
| 11006    | Returned RADIUS Access-Challenge                                            |
| 11001    | Received RADIUS Access-Request                                              |
| 11018    | RADIUS is re-using an existing session                                      |
| 12504    | Extracted EAP-Response containing EAP-TLS challen                           |
| 11006    | Returned RADIUS Access-Challenge                                            |
| 11001    | Received RADIUS Access-Request                                              |
| 11018    | RADIUS is re-using an existing session                                      |
| 12504    | Extracted EAP-Response containing EAP-TLS challen                           |
| 12505    | Pre-processed EAP-Request containing another EAP-TLS challenge              |
| 11006    | Returned RADIUS Access-Challenge                                            |
| 11001    | Received RADIUS Access-Request                                              |
| 11018    | RADIUS is re-using an existing session                                      |
| 12504    | Extracted EAP-Response containing EAP-TLS challen                           |
| 12505    | Pre-processed EAP-Request containing another EAP-TLS challenge              |

Table-3: Table shows the sequential events during the authentication process.

In this state BYOD-Trusted-Employee user is accepted after completion of the authentication and the devices COA(Change of authorization) triggered. Post COA the device will get Post-auth IP address from isolated network, which will directly go to the internet through external Firewall.

Implication and security risk even after this isolated environment is if the External Network Internet is used as the same Internet exit path of the enterprise. If the enterprise has APNIC IP address registered
BYOD Secured Solution Framework

then any malicious activity done by the BYOD user will be
the responsibility of the enterprise. This study highlight and
suggest to use a different Internet exit path apart from
corporate Internet.

The 2nd risk also can occur with Cloud services if corporate
IP is used for BYOD user. The ideal case of any enterprise
cloud services is creating NSG in cloud for accepting traffic
from enterprise Public IP segment. Incase if this use same IP
segment then BYOD users will get access to the enterprise
termed infrastructure hosted in cloud. So this study explored
the risk of cloud services so suggest to use different Public
IP-separate isolated public network to build a secure
infrastructure.

3.A Monitoring of the BYOD-User activity and Audit
compliance

Monitoring of the activities using Public IP as per the IP
address retention and use Policy, Lawful disclosure[11] for
services provider is mandate to manage the logs. In the case
of any malicious activities logs has to be maintained incase
of any dispute and investigation situation Service provider
will directly identify the IP assigned organization. In this
case user identification will be the responsibility of the
test while ISP will only identify the enterprise where
Public IP released. User acceptance policy also need to be
agreed and signed by the BYOD user as per organization
security policy framework measurement.[4]

Monitoring of the BYOD users activity is a major concern,
so BYOD solution should have proper log management
model to capture logs and identification of the users, and
storing such large amount of logs.

In this research Cisco Identity service[12] solution is used in
connection with additional user database as active directory
used while Aruba CPPM Clearpass Policy manager[13] solution
is also one the solution to manage logs. ARUBA
CPPM which is also use for the IOT, Mobile devices and
access management, which works in role base access model.
But either Cisco or Aruba both solution does not comply the
enterprise security and audit requirement, which is enterprise
responsibility. So this study address the complete end to end
requirement while enabling BYOD and maintain security
compliance.

3.B CASE-2: BYOD-Untrusted-User: Not active
Directory user

The use case of this type of Wireless access is generally
provided to untrusted users who are normally visitor to the
organization. In such case user id created using Lobby
administrator portal, or self sign in method which is normally
a AAA server use model. In this case Guest user id get
created with some time duration or permanent duration. This
situation can be addresses if AAA server is local to the
branch. But security challenges comes when AAA server is
not local.

3.C CASE-3: BYOD-Untrusted-User: Not active
Directory user and user is located in Remote Branch and
AAA server is centralized.

The design of the BYOD architecture impact to cost. The
major cost of the BYOD are Hardware,[14] software,
Bandwidth, Network and Operation.

Different deployment model approach cost are different.
While CIO of the organization initiate the project, always
cost benefit analysis happened and design approach also get
optimized.

One of the cost saving model is centralized architecture and
in this test AAA server is placed in Centralized location and
BYOD-untrusted user located in remote Branch over MPLS.
This use case is tested to save the cost of the deployment and
overall project cost.

IV. DISCUSSION

This research study and design framework has a major
advantage for the BYOD-Trusted-Employee as if any
employee travel across any other Branch office of the
organization will have seamless access of BYOD internet
services, as certificate based authentication is used and
seamless onboarding process and secured method of BYOD
access. SSID has to be same and same AAA is used and
central method of authentication even this can be in
distributed architecture.

A. Contribution

Main contribution of this study after analyzing the traffic
routing requirement from BYOD users devices to the AAA
server is how BYOD design architecture should be to reduce
security risk of the organization.

BYOD-Trusted-Users who are basically active directory
users authentication model, authentication mechanism and
onboarding process without any risk of the organization laid
down security framework. 2nd type of the users BYOD-
untrusted-users who are not organization active directory
users are the biggest challenging onboarding, which need to
be taken care with additional security parameter. In the 2nd
case of BYOD users authentication ideally recommended to
have easy onboarding process but with additional security
measure.

The risk of onboarding 2nd category BYOD user is their
authentication mechanism, in such situation initially devices
gets the IP address which is pre-auth IP, in-order to
authenticate this devices, Pre-auth IP need to have IP
reachability to the AAA server or controller should have
proxy the traffic to AAA server. The organization
recommended secured design model suggest devices pre-
auth IP should be directly to external network, but in this
case authentication request does not proxied to AAA server
which is in trusted zone. Guest user pre-auth traffic should
not be routed to design secure infra.

Process for Authentication as

When BYODE AR  AAA

If BYOD User==AD

Then ADR=Success else ADR=False

IF ADR = True then AASR  WLC for Post-auth.

To overcome such situation and reduce the risk of routing
untrusted IP network in trusted MPLS/LAN zone, external
encrypted tunnelled to be created from Branch office
Untrusted Guest Internet zone to Data center Guest internet
zone.

Internet Access revoke from BYOD also one of the major
attention point. In this solution this is been tested while the
employee gets deactivitated from Active directory, then
certificate gets expired and reauthentication request get failed
thus security compliance is maintained 3rd category of the
corporate wireless users does not have any such challenges
as their wireless Controller and AAA servers resides in
trusted Network and same

Wireless Access points are

used.

Retrieval Number F8202088619/20190@BEIESP
DOI: 10.35940/ijeat.F8202.088619
Published By:
Blue Eyes Intelligence Engineering & Sciences Publication
This study contributes to create a secured framework of the BYOD implementation in centralized and distributed model. While keeping all organization security policy.

B. Implication
This study highlight the BYOD design that Cost factor which is one of the major direction before adopting the BYOD solution. Since this service is an employee satisfaction category service in work environment so every CIO of the organization looks for reducing the cost. But in saving the cost major risk can get involved in security compliance.

Selecting the BYOD design depends on the organization security framework strength

C. Future study
This study explored and suggest that more analysis required in BYOD environment in connection of Cloud Security. In Traditional BYOD design does not have cloud security analyses. But since cloud adoption is exponentially growing and BYOD traffic exits from same gateway in ideal case, so BYOD design and cloud security with Software define WAN need to studied in depth

V. CONCLUSION
Organization need to address the security risk while giving the internet access to employee on their personal devices from corporate wireless infrastructure.

It is not possible to segregate wireless access point and wireless Lan controller for Corporate intranet wireless and BYOD wireless in same physical area. Co-channel interference and adjacent channel interference lead into major interruption of services in RF Media. So in this study multiple SSID broadcasted in same area using same AP, Controller for BYOD services in secured way. While giving the internet access using same controller and Access point, security model must be designed in such a way so that end to end traffic segregation is maintained.

In this study, it is demonstrated that BYOD service to be divided as Two different profiles. Firstly for BYOD corporate user profile which is a Trusted User Profile. It is demonstrated to be a certificate based authentication which can be recommended as secured model. And Secondly for guest access which is Untrusted Profile, it is recommended to have Layer three open authentication.

In either of the case it is recommended to have the gateway of the BYOD devices outside the corporate LAN infrastructure, which can be considered as best secured way of managing BYOD infrastructure. Even if the personal devices are connected to the same Wireless Access point but the gateway of the BYOD devices should be outside the DMZ Firewall as referred in Figure 1 which Segregates LAN and External Segment and maintain secured way of access.

This study demonstrated a very secured model of traffic flow of BYOD, before even getting the Pre-authentication IP address, traffic is encrypted with EAP tunnel and landed directly outside corporate LAN. In this scenario this is analysed that BYOD (Both type of SSID) vlan does not even required to be created in corporate Core LAN infrastructure. even there is no requirement of Routing of those BYOD IP segment inside LAN. This makes Corporate LAN infrastructure secured while giving internet access to BYOD user.

BYOD access management and revoking of Internet access as an exit management process which is very large numbers in bigger organization also becomes automatic with this mechanism of BYOD architecture, which protect organization from security risk and becomes system driven process rather manual intervention.

This study also analyse one important direction of designing the BYOD and cloud security architecture and risk, and mitigation towards today’s demand cloud services adoption.

REFERENCES
1. Z. Mitrovic, I. Veljovic, G. Whyte, and K. Thompson, “Introducing BYOD in an organisation: the risk and customer services viewpoints,” p. 26, 2014.
2. P. K. Gajar, A. Ghosh, and S. Rai, “BRING YOUR OWN DEVICE (BYOD): SECURITY RISKS AND MITIGATING STRATEGIES,” p. 9, 2010.
3. C. Walker-Osborn, S. Mann, and V. Mann, “to Byod or ... not to Byod,” ITNOW, vol. 55, no. 1, pp. 38–39, Mar. 2013.
4. C. Z. Tu, J. Adkins, and G. Y. Zhao, “Complying with BYOD Security Policies: A Moderation Model Based on Protection Motivation Theory,” Journal of the Midwest Association for Information Systems, vol. 2019, no. 1, p. 19, 2019.
5. P. Baillette, Y. Barlette, and A. Leclercq-Vandelannoitte, “Bring your own device in organizations: Extending the reversed IT adoption logic to security paradoxes for CEOs and end users,” International Journal of Information Management, vol. 43, pp. 76–84, Dec. 2018.
6. J. Allen and J. Wilson, “Securing a Wireless Network,” p. 3.
7. L. Maccari, R. Fantacci, T. Pecorella, and F. Frosali, “Secure, fast handoff techniques for 802.1X based wireless network,” in 2006 IEEE International Conference on Communications, Istanbul, 2006, pp. 3917–3922.
8. K. W. Miller, J. Voas, and G. F. Hurlburt, “BYOD: Security and Privacy Considerations,” IT Professional, vol. 14, no. 5, pp. 53–55, Sep. 2012.
9. [M. Ph. Stoecklin et al., “Passive security intelligence to analyze the security risks of mobile/BYOD activities,” IBM Journal of Research and Development, vol. 60, no. 4, pp. 9:1–9:13, Jul. 2016.
10. Yong Wang, Jinpeng Wei, and K. Vangury, “Bring your own device security issues and challenges,” in 2014 IEEE 11th Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, 2014, pp. 80–85.
11. P. Iyengar, “IP ADDRESSES AND EXPEDITIOUS DISCLOSURE OF ENTITY IN INDIA,” vol. 9, p. 28.
12. S. Jose, “Cisco Identity Services Engine Administrator Guide, Release 2.2,” p. 1240.
13. P. Kaspiyan, “ARUBA CLEARPASS NETWORK ACCESS CONTROL,” p. 5.
14. J. Loucks, R. Medcalf, L. Buckalew, and F. Faria, “An astounding 89 percent of companies are enabling their employees to use their own devices for work purposes,” Economic Analysis, p. 26.

AUTHORS PROFILE
Md Iman Ali is a Research scholar. in the department of computer application at Lovely Professional University, Punjab, India. He has completed MCA and DOEACC “A” level. As a professional certification he is CCIE Lab certified. His research interest area include BYOD secured solutions, Cyber security, SD-WAN Security, Cloud Security and Smart city Cyber Forensic.

Dr Sukhviran deep Kaur, is an assistant professor in LPU, Punjab, India. She has received PhD from NIT, Srinagar, India. Her current research interest includes Cyber Security, BYOD solutions, Forensic Science.