Bring Your Own Device

To BYOD or not to BYOD

Akshay Deshpande[#1], Amber Nighojkar[#2], Dhruvin Mehta[#3], Sameer Singh[#4]

[#]*Information Security Management, Symbiosis Centre for Information Technology*
Plot 15, Phase-I, Rajiv Gandhi InfoTech Park, Hinjewadi, Pune - 411057, Maharashtra, India.

[1]akshay.deshpande@associates.scit.edu

[2]amber.nighojkar@associates.scit.edu

[3]dhruvin.mehta@associates.scit.edu

[4]sameer.singh@associates.scit.edu

Abstract— **BYOD is the new buzz word in the industry. Almost all the big players are aiming to utilize this lucrative concept for cutting their costs and maximizing the profit. Companies are trying to survey the employee owned devices and cut their own expenditure on assets. This concept is specially a boon for small and medium sized organizations; as they can cut down on their costs exponentially by letting the employees' access the corporate data on their own devices.**

Affinity towards BYOD is easy to justify. Smart phones, tablets and other devices provide a level of access and convenience that was never imagined before.

Prima facie two major issues are - Security and Manageability. Use of personal devices makes the infrastructure exposed and vulnerable to viruses and other cyber-attacks. Also, it is easy to compromise data if the device is stolen. Another big challenge is to manage a large pool of diversified devices. It is a tedious task to find a platform which can accommodate all these devices.

Through this research paper, we identify the various problems that the organizations could face in BYOD environment and provide the solutions that can mitigate them.

Keywords— **BYOD, Security, Data, Risk, Controls, Solutions**

I. INTRODUCTION

Bring Your Own Device (BYOD) permits employees to bring personally owned mobile devices to their workplace and use those devices to access company information and applications. It is an alternative strategy that allows employees, business partners and other users to utilize a personally selected and purchased client device to execute enterprise applications and access data. Devices that come under the purview of BYOD are laptops, smart phones and tablets.

Employees wish to use their own devices to view work e-mails while on the move, access work files from company servers, access internet for work purposes, use publicly available apps for work related activity and company provided apps for approvals and requests.

A few advantages of BYOD: Higher job completion rates, reduced paperwork, improved customer service and response time, increased productivity and efficiency, more accurate billing and record keeping, increased customer satisfaction, reduced sales cycle, reduced liabilities, reduced operational costs and improved data collection and accuracy.

Spurred on by the consumerization of IT, BYOD is here to stay, particularly as employees continue to favor the flexibility and usability of their own devices (Figure 1). As a result, companies can no longer afford to ask whether or not they should BYOD. Instead, they must determine how to enable BYOD in a way that mitigates its risks and creates value for the entire enterprise.

One way ahead is to go for investment in the tools, solutions and practices required to support BYOD, organizations can mature their technology and infrastructure capabilities to deliver IT services more efficiently and effectively.

Employees across the board are well aware of these benefits and are increasingly demanding their employers provide them with more advanced and high-tech mobile devices, more power of choice and increased control over their own devices, and access to more mobile-friendly enterprise applications. So generally users want to carry a single device which may be provided by the employer or may be bought be themselves as per their needs. Allowing this will greatly improve employee morale and also boost the productivity.

Fig. 1 BYOD Acceptance Data

II. PROBLEM DEFINITION

Although BYOD is the new face of mobile consumerization, numerous challenges follow in its wake, ranging from human resource (HR) and legal issues to compliance and security risks. Due to no industry wide BYOD standardization, organizations can expect to have a few challenges.

Each device may it be tablet or smart phone brings with it a whole new set of challenges which need to be handled. The IT department will need to keep a track of all the devices that wish to access the corporate network and only after it is deemed safe can it be allowed to be used. All of this can add a lot of overhead to the IT staff, not to mention additional risk of a security breach. Also client side security requirements may create a conflict in implementing a BYOD policy in place.

Additionally, allowing employee-owned devices to access corporate e-mail servers, file storage servers, applications servers, and the like will quickly result in a device filled with proprietary information, so the program needs to reduce and prevent risks posed by devices that are lost or stolen. Moreover, if the device contains both corporate and well as employee personal data, there may be legal impacts of back-up or wiping personal data. Monitoring employee-owned devices for authorized use, and enforcing the use of defined policies, can also be a challenge in practice.

Any strategies for overcoming these challenges must take into account global variations in regulations regarding personal data privacy and employee monitoring. Also there would major issues related to support and maintenance.

A BYOD policy can result in a hodgepodge of mobile device with a variety different operating systems resulting in an increase in the likelihood of application incompatibilities. Even with the introduction of a BYOD policy, IT will be involved in deciding which devices will be supported and which won't – and consider how to cost-effectively develop and support secure business applications across a variety of platforms. The situation is worsened by the very fact that operating system upgrades for these mobile devices will likely take place outside the control of IT. Additionally, employees will be downloading many of their applications from public-facing Internet application e-stores. Setting up your own proprietary applications along with third-party public services – and keeping those enterprise applications private will be needed to be done carefully.

A broader array of devices and mobile operating systems can also substantially increase the IT support burden if not carefully managed. IT needs to determine a reasonable level of support for BYOD to sufficiently meet the needs of end users and that of the company. IT should also to some extent be expected by employees to impose certain non-negotiable centralized mobile device management requirements and capabilities for any device touching corporate systems. Apart from the device support and cost there will also be cost related to the data plan. This will be additional financial exposure to the company. Also there would be some who would not be so keen to adopt the BYOD policy. In such a case there will have to be incentives that need to be given to these people in order to make sure all comply with the policy. If there is any gap, then there will be serious consequences to the security posture of the organization.

Problem 1:

Present day smart phones are not designed with enterprises at the center. Further, the BYOD trend imposes employees' use of their personal mobile devices.

To deal with BYOD, companies are using third-party applications and containers onto employees' personal devices. It calls for installing security and management controls. These solutions are temporary and aren't good enough to meet the true needs of either the enterprise or the employee. They cannot address all the requirements and pose following issues:

- Security risks from malware
- Data leakage
- Proprietary systems come with management complexities

Problem 2:

Another problem with BYOD devices is the underlying kernel. When the device has been provided by corporate, then the firm has a control over the OS, kernel and configurations that are installed which is not the case in employee owned devices. This results in a major security challenge. The problem is further increased when employees (purposefully or accidently) alter device settings to bypass security policies.

Problem 3:

The devices brought-in by the employees & guests for ease of access to work related information and data can turn out to be a threat to organization's IT security. One of the problems that arise due to BYOD implementation is network access issues of the organization.

The key challenges are:

- Differentiation between corporate, employee and guest networks so that users can only access authorized applications
- Reduction of time consuming registration process of each device when it tries to connect to the corporate network
- Ensuring a capable performance network to support a huge number of devices that are trying to connect to organization's network concurrently

Problem 4:

When the higher management has gone for the decision of going for a BYOD policy, they need to take in account the various stakeholders and the considerations and possible impact of this BYOD strategy on these stakeholders. Often the first to be taken into consideration is the Legal department.

We need to ask questions like:

- How can the local privacy and data protection regulations impact the implementation of BYOD strategy?
- If organization is implementing in every country, what can be done to not have to start from scratch in every country being targeted for implementation?
- What are the different contracts that need to be created by the legal department?

Next comes the Human Resources department. It is a key stake holder and plays the role of centralized awareness system in order for the smooth implementation of the BYOD strategy.

We need to ask questions like:

- How does BYOD policy affect hiring and firing policies?
- How should the training and awareness of the employees be handled due to the BYOD policy in picture?
- How to handle a situation of breach of policy like installing unapproved applications? What are the next steps that need to be taken?
- What happens when a person who was using his personal device for official purposes, quits?

Next comes the Finance considerations. Often, the main driver of BYOD policy is cost saving, but what about the maintenance and providing corporate bandwidth and other resources. A proper policy needs to be in place to tell about what costs will be covered and what will not be covered as part of the BYOD strategy.

We need to ask questions like:

- Who is responsible for the cost of buying the device and future repair costs?
- If there is a need for a voice and data plan, then the costs for it will be covered by the company or employee?
- Who will be paying for additional charges like roaming?
- Who will pay for the accessories that one needs with the devices?
- What about the cost of providing support for these devices, who is responsible for that?

Last are the IT considerations. These form the backbone of the implementation of the BYOD strategy. Without them, the various steps of rollout, implementation and providing security cannot be achieved.

- What are various types of devices that will be supported?
- What are the various OS's that will be supported?
- How will jail-broken or rooted devices be handled?
- How to manage the initial rollout? Should it be pilot or should it be an enterprise level implementation throughout?
- How to ensure the compliance with the BYOD policy that was put in place?
- How to handle OS, App upgrades?
- If an employee loses a device, should IT wipe the entire device or only the corporate data part?

III. APPROACHES TO SOLVE THE PROBLEM

As organizations ride the BYOD tsunami and launch initiatives to tame it, structured approaches are few and far between. If organizations hope to reach both their short and long term objectives, they have to adopt a multi-tiered approach that addresses key BYOD challenges.

Key BYOD considerations: (Figure 2)

Define BYOD objectives-

- Align BYOD objectives with the overall strategy
- Decide on a position: cost reduction vs. increased productivity vs. risk mitigation

Fig. 2 BYOD Pyramid

Evaluate Risks-

- Identify both the internal as well as external risks that can impact the success of the BYOD program
- What is the amount of existing personal device penetration in the organization? What regulatory risks are existing?
- What are the possible implications to the organization?

Define Policy-

- Effective BYOD programs require enterprise wide collaboration (i.e. Finance, HR and Legal).
- Some of the key policy criteria's include eligibility, support, reimbursement, policy violations etc.

Operationalize and Implement-

- Identify and analyze available vendor solutions based on alignment with objectives and policies
- Streamlined device certification is key to providing timely access

Mitigation:

Create a BYOD policy that outlines the rules of engagement and states the company's expectations. The policy should also state and define minimum security requirements and may even mandate company-sanctioned security tools. Separate the personal and corporate data. Have a strong password policy in place for each device.

Protect all highly sensitive servers with multifactor authentication. Use sandboxed applications which houses corporate data into a separate container that can be secured with passwords and other authentication mechanisms; non-business data should be kept separate so that users can continue to use their devices for personal use.

Maintain secure access to the corporate network by establishing the minimum security baseline that any device must meet to be used on the corporate network, including Wi-Fi security, virtual private network (VPN) access and any add-on software to protect against malware. It is also critical to identify each device connected to the network and authenticate both the device and the person using the device. Make it mandatory that IT has admin privileges on all devices connecting to corporate network. Require all employees to have anti-malware software installed on the device and automatically deny access to any that do not. Insert application-level filtering of traffic to inspect BYOD traffic to the corporate network to ensure no malware or exploits pass from the BYOD segment to corporate servers.

Create a policy on BYOD which incorporates mandatory regulatory compliance and data privacy related laws and regulations. Virtualization solution such as Virtual Desktop Infrastructure (VDI) can be used since it removes the limitations of maintaining a stringent acceptable client list for an organization and allows end users to use their preferred devices that ultimately connect back into a managed VDI. Chalking out a white list of properly vetted apps can ensure that blacklisted apps cannot be downloaded on the devices.

Solution to Problem 1:
Use BYOD devices that provide:

- Strongest security
- Best demarcation between corporate and personal data
- Best management tools (Figure 3)

This will assure consumers that their personal content and device usage will remain private and unaffected by their employer's BYOD policies. (Figure 4)

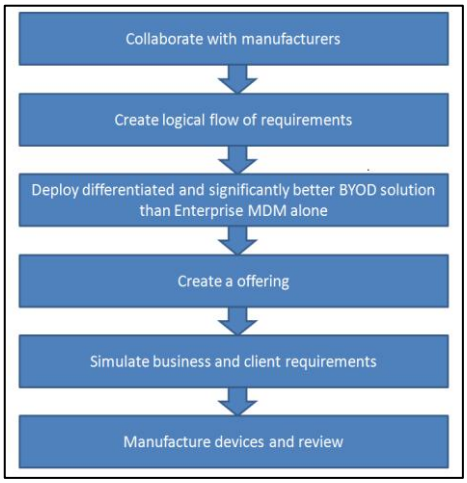

Fig. 3 Logical flow diagram for implementation

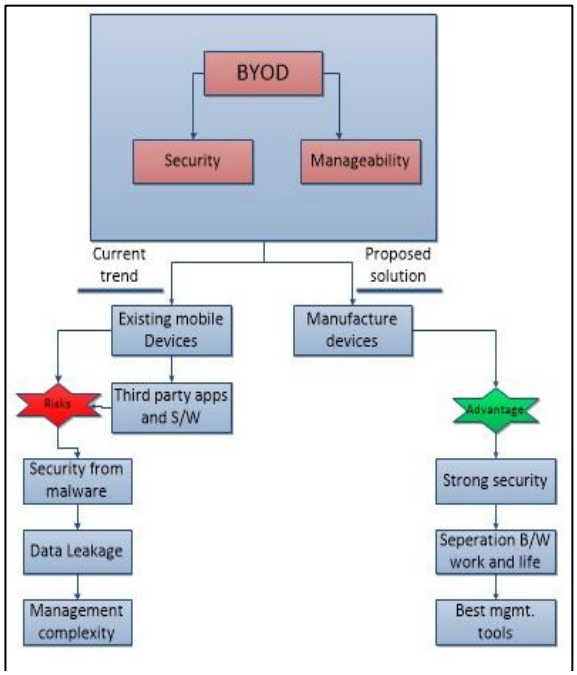

Fig. 4 Design Flow Diagram

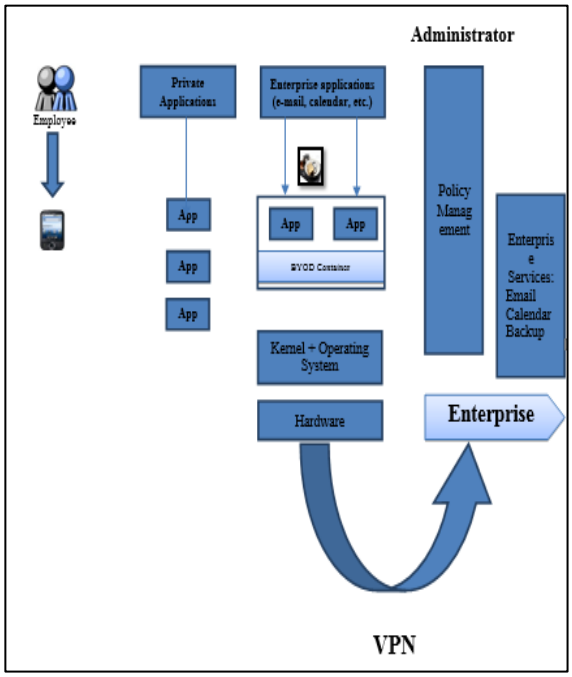

Fig. 5 Architecture of proposed solution

Solution to Problem 2: (Figure 5)

The solution is to be able to secure the mobile device without having to alter the device OS and software and still make sure the device is safe enough for the corporate network and data. This solution will strengthen and isolate the execution of enterprise applications.

There are currently many solutions in the market that are based on virtualization and other specialized applications. But all of these require changing the OS and its configurations. The solution that we will provide is flexible as there are no changes required to the device and it will concentrate only on the corporate data and keep the employee's data in its own discretion.

Finally we will also discuss a complementary policy management and enforcement procedure using an effective MDM (Mobile Device Management) layer.

Our solution consists of deploying a container inside the user application space in the mobile device. The container is installed in the user level application space.

The application container consists of a set of interceptors which are used for both native and java function calls from the application to the system.

The container loads the application in such a way that critical function calls outside the application, to libraries or system calls, are replaced by our own stubs. Stubs provide the extra functionality of performing encryption on write. The stubs also help to allow or deny calls from the application when corporate data comes into picture. Also the corporate data and network can only be accessed via the container.

We can use security protocols for encryption and the keys can be securely stored in tamper proof storage. The keys would be kept separate in such a way that they are not accessible to any attacker. We can also put a mechanism to generate session level keys, so that even if the attacker gains the access it will only be for a specific period.

Also the policy management can be enforced by the administrator and can be made sure that the corporate data is kept safe. Along with the control over the access that stubs provide, it also can help the administrator to perform Remote wipe, secure data storage and fine-granular policy management.

Our solution gives the IT administrators of organizations privilege to tweak the security parameters as per the security requirements of the organization.

If implemented with all the features, this solution is highly scalable, efficient and can be easily integrated in small, medium and large-size industries.

Solution to Problem 3:

To differentiate between different types of networks, a "SSID-driven network" approach is followed. The organization's network can broadcast three different SSIDs in following manner: (Figure 6)

- The first SSID is totally dedicated to corporate devices for authentication of employees
- The second one is "Guest SSID" which allows employees to connect to corporate network with their own devices. This is basically done to allow users to download wireless configurations for having an access to BYOD SSID
- The third secure SSID is "BYOD SSID" which is used to allow employees for logging in to corporate network securely

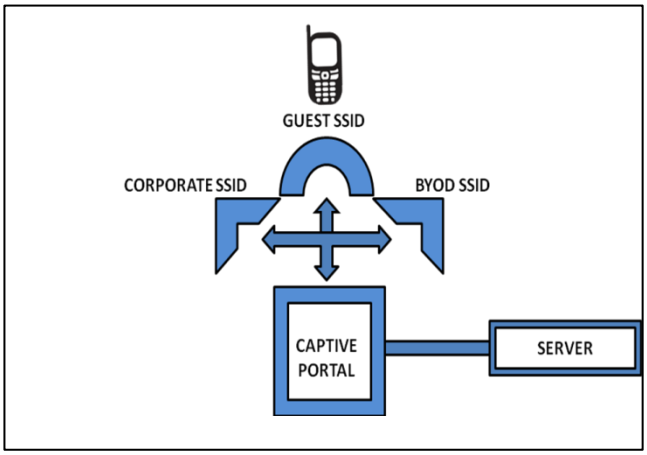

Fig. 6 Architecture of proposed solution

To eliminate the process of registration of each device on organization's network, the use of captive portals can be taken into consideration. The only requirement is to have a valid username and password from network administrator of the company. After the user logs in, the certificates are downloaded and device gets automatically configured for access to BYOD SSID.

In order to ensure a better performing network to support large number of devices, a huge bandwidth with state-of-art infrastructure must be used.

Solution to Problem 4:

A decision to implement a BYOD model involves many stakeholders and decisions. These key takeaways should be considered by an organization when planning the approach:

- Identify the main benefits that the company will obtain from the BYOD model
- Identify the important stakeholders and obtain their support
- Have a formal executive sponsorship process
- Create a set of formal policies that consider all aspects of the BYOD program

IV. CASE SCENARIO

Crystal Technologies is a Mumbai based mid-sized IT solutions firm specializing in finance domain. It was founded in the year 2001 and since then has grown in size and reputation. Its employee base currently stands at 10,000 with branches around the world. It has clients from various industry verticals but with its specialty in finance domain, its major clients were primarily banks, brokerage firms, hedge funds and other financial institutions.

In the year 2010, a major bank came to Crystal with a requirement for developing a net banking solution for them. It was a big client for Crystal and a lot of revenue was to be gained. But with the criticality of the project, there were a lot of restrictions on the data of the project. A lot of security was needed due to the sensitivity of the data. The service level agreement required Crystal Technologies to comply with various security requirements. The initial project team was appointed with great fanfare and the project kick started in December 2010. Mr. Mehra was selected as a senior programmer then. Over the years the project was running smoothly, and after delivering the initial set of functionality, the project scope was expanded to include more functionality. Mobile banking, online banking and other features were made as part of the subsequent releases. Mr. Mehra performed very well and greatly impressed the client. Due to the complexity of the project the team had to sometimes spend long hours. Increased functionality required more skills and the company sometimes had to bring in consultants on contract from outside for some areas where there were no resources available in the company with those skill sets. The company generally did not report this to the client as they did not want the client to know about their lack of capability in those areas.

Mr. Mehra was promoted to Assistant Manager in 2013. By this time he was aware of the in and out of the project. He had a good relationship with the clients and his team members. Being a critical resource of the project, he had a clear idea about the various parts of the project. He had the responsibility of handling the payment gateway solution and the requirement gathering process. Because of this, he had to travel a lot especially to client locations. He had a lot of client interactions and always was required to have data on the go. In order

tomanage this information and data, he was provided with a laptop. He used to work from home as well as client location with this laptop. The company had installed a host based antivirus program on each of the company laptops which used to get updated with the latest virus definitions and security patches on a weekly basis.

Mr. Vadra worked as an independent consultant and specialized in designing payment gateway for online payments. He used to work on contract for various companies due to his unique skill set. Before working as an independent consultant he used to work for a leading bank.

In April 2013 as part of a functionality related to online banking, Crystal Technologies hired Mr. Vadra. He was to work with Mr. Mehra as to obtain the initial requirements for the specific functionality.

By this time the project was going well and Mr. Mehra was responsible for a lot of things. He was sometimes getting a bit overloaded with work and was frustrated as he had to be aware of all the things going on in the project. Whenever the client needed some clarification about some requirement, he had to access his laptop and corporate network as it was not possible for him to remember everything. During travelling it was especially very inconvenient as he needed the information quickly.

Mr. Mehra, in order to make his life easier decided to transfer some of the client data to his smartphone for ease of access anytime and anywhere. He also transferred the details of the requirement documents of future functionalities in pipeline as there were still discussions going on regarding them with the client. Further, he transferred payment gateway design architectures complaint to PCIDSS V3.0 to his smartphone as there were some major changes required due to recent security demands of the client. Because of the ease with which he used to access most of the documents from his smartphone, he did not connect his laptop to the corporate network as most the data was available from his phone only.

Mr. Vadra came to know of Mr. Mehra's practice of transferring the data to his phone. He told Mr. Mehra that he wanted the same privileges and if Mr. Mehra disagrees, Mr. Vadra would report it to the higher management. Mr. Mehra, fearing the consequences allowed Mr. Vadra to transfer the data as he felt there was not much harm in this.

In September 2013, it was a regular day at office and Mr. Mehra was working on the latest requirements sent from the client. Just then he got a call from the network team informing that he was called to the conference room for an emergency meeting. He went to the meeting and was shocked to know that there was a major security breach. The network servers were infected with malware and it was resulting in denial of service attack on the corporate servers. Also the network team were worried that the data was being transferred from the servers to a remote location. An attack of this magnitude was a major issue for Crystal Technologies.

In the morning that day Mr. Mehra had connected his smartphone to his laptop. He had used this phone for his personal usage like browsing the internet and also had installed various applications on it. During such browsing sessions, a latest malware infected his phone and when he connected his phone to the laptop, it got transferred to the laptop as well. As Mr. Mehra did not use his laptop for frequent periods, it was not updated with the latest virus definitions and was unable to detect this malware. The laptop when connected to the corporate network spread through the network. Mr. Mehra was completely unaware of this until the security incident happened.

There was complete chaos and the network was completely down which led to major security breaches. In all this mess, the project came to a stand-still. Mr. Vadra was done with his contract and had left the company with the data. Mr. Mehra, already under investigation for the security incident did not tell about the data on Mr. Vadra's phone as well. A high level meeting was held the next day and Mr. Mehra was relieved of his duties from the company.

TABLE I. RISKS AND MITIGATION

Sr.No	***Risk***	***Mitigation***
1	No BYOD Policy	Create a BYOD policy that outlines the rules of engagement and states the company's expectations. The policy should also state and define minimum security requirements and may even mandate company-sanctioned security tools. Security policy initiatives might include limiting activities that employees are allowed to perform on these devices at work and periodic IT audits to ensure the device is in compliance with the company's BYOD security policy.
2	Data disclosure	At the end of the tenure of an employee either a full time or contractual, all the devices must be checked and must be cleaned of all client confidential data.
3	Unsecured network access	Maintain secure access to the corporate network by establishing the minimum security baseline that any device must meet to be used on the corporate network, including Wi-Fi security, virtual private network (VPN) access and any add-on software to protect against malware. It is also critical to identify each device connected to the network and authenticate both the device and the person using the device. (Figure 7) Implement a custom device-enrolment program, which will limit the number of devices per employee and will give an accurate view of who's accessing the network at any given time.
4	Introduction of malware to corporate servers	Make it mandatory that IT has admin privileges on all devices connecting to corporate network. Require all employees to have anti-malware software installed on the device and automatically deny access to any that do not. Insert application-level filtering of traffic to inspect BYOD traffic to the corporate network to ensure no malware or exploits pass from the BYOD segment to corporate servers.
5	Gaps in recruitment process	Processes for doing the background check of resources hired on contract

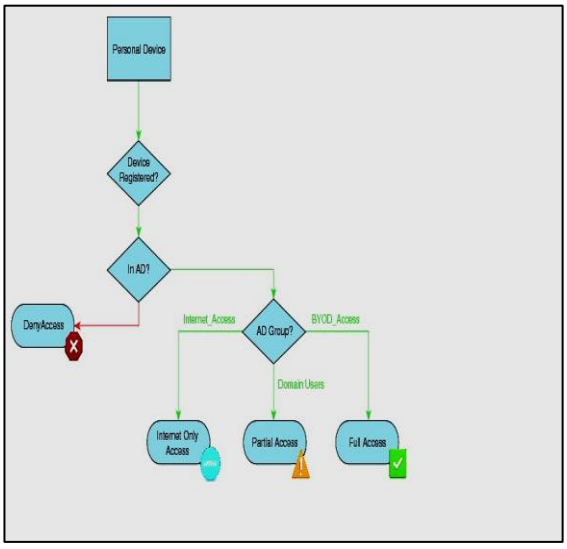

Fig. 7 Process flow of BYOD authentication

V. DRAWBACKS OF THE PROPOSED WORK

There are a couple of issues with the solutions explained before. Primary issue being is a tedious task to convince enterprises, vendors and employees. Enterprises will be initially hesitant regarding the success as employees might not show an interest in using these devices which can cause a huge financial loss to an enterprise. Vendors will not be ready to manufacture customized devices until there is a minimum order which can assure them profit. Also, it will be challenging for the vendors as different organizations will have different requirements. Generally, the employees have a smart phone of their own. They might also not be satisfied with the features provided in the enterprise customized phones as it will be designed specifically to cater to business requirements. Another drawback is that vendor should be able to satisfy the requirements asked by the enterprise. It will also take efforts to assure top management about the success of this solution as it will require huge monetary investment. It may not be appropriate for small and medium organizations.

In case of stubs, drawbacks here are that the system will be updated as per the way the latest applications are present in the enterprise. The stubs need to be able to handle a variety of threats that come its way. The administrator needs to be able to handle a large number of varieties of phones and each brings with itself thousands of apps which can possibly cause harm to the corporate infrastructure. The administrator must be updated about the latest software patches and OS configuration and also be proficient in the design and management of stubs. Also, the user makes sure the BYOD container is the single pathway to the corporate data and installed apps. If the BYOD user does not properly follow the policies set by the administrator and abuses the system then there is scope for security issues. These need to be addressed at the earliest.

The BYOD container which has to be installed in each and every BYOD device is a big administrative task as it has to be correctly configured as per the requirements, without which the purpose of the solution will fail. Also, once the configuration and updating is done, there needs to be periodic maintenance to make sure container is up to date and is best configured to protect the network of the organization. For a variety of devices it needs to be compatible. Hence, it is essential to take care of all these issues when it comes to the implementation for a large user base.

VI. CONCLUSIONS

Gartner claims that BYOD adoption is most common in mid-to-large enterprises which have anywhere ranging from around 2,500 to 5,000 employees, with US firms more likely to embrace the trend than their European counterparts. Nearly 40 percent of CIOs expect to stop giving workers corporate-owned devices by 2016. By 2017, the firm expects half of companies to require employee to provide their own device at work.

- Top BYOD benefits to companies are increased productivity, increase in employee satisfaction and reduced costs
- The drive for BYOD is that employees want the choice of device, applications, and ability to combine personal and work lives
- Transformative benefit of BYOD is employee-driven innovation - by allowing employees to finalize how exactly, when, and with which available tools work is to be completed, companies will be able to unleash a wave that adds value to the organization
- BYOD, however, implies new challenges in security and IT support
- Companies must be proactive to solve the challenges of BYOD with improved mobile policy and cost-reduction strategies

VII. FUTURE WORK

Organizations are gradually moving towards this solution as they find it suiting their requirements. Many organizations have already started adopting this solution. One example is Hewlett-Packard which had launched a tablet for its employees with its own customized operating system. Also, many mediator companies have also emerged which act as a bridge between the enterprises and the vendors.

A lot of work and research is being carried out in this area by a lot of people and soon we may be seeing this solution implemented in many more organizations.

The area that needs to be targeted for further innovation and research here is to create a sort of template and a modular container that can be able to have a single setup that can be configured on any device. The advantage here would be the

massive reduction in the maintenance work and other overheads that come in to picture due to the implementation of this solution.

Also there needs to be a centralized control process which can monitor, update and handle any issues that are caught. The stubs and their configurations need to be able to control from here. We can have remote wipe or blockage of access for specific devices. We can block all the traffic if we can control the BYOD container.

Hence future work would involve trying to improve, make easy and more secure via better and more efficient administration. For this to happen, a lot of research in the BYOD container design needs to take place before an exact solution be obtained.

ACKNOWLEDGMENT

This research project has been made possible with the help and support from everyone, including teachers, peers and friends. We would like to dedicate our acknowledgment of gratitude towards the following significant advisers and contributors:

First and foremost, we would like to thank our project guide and mentor, Dr. Ganesh B. Janvale for his continual support and encouragement. He guided us at each and every stage of our research and gave valuable suggestions, advice and direction towards achieving the objectives of this project.

Without his supervision, this project would have not been possible to finish.

We would like to show our gratitude to our college Lab Team members for providing the necessary equipment and infrastructure that aided our research and helped in our project.

Furthermore, we sincerely thank all our peers and friends, who provided valuable advice and support at significant steps of our research.

REFERENCES

[1] Sam Ganga, "BYOD: Six tips for a successful implementation", http://www.datacenterjournal.com/it/byod-tips-successful-implementation/, Oct 7, 2013.

[2] Jaspreet Singh, "4 Keys to Creating a BYOD Program", http://www.securitymagazine.com/articles/84771-keys-to-creating-a-byod-program?v=preview, January 10, 2014.

[3] Security 500 "BYOD Users Expected to Double by 2014", http://www.securitymagazine.com/articles/83388-byod-users-expected-to-double-by-2014, January 10, 2014.

[4] Security 500 "Study: IT Leaders Approve of BYOD", http://www.securitymagazine.com/articles/83092-study--it-leaders-approve-of-byod, January 10, 2014.

[5] Bring Your Own Device (BYOD) Policy Guidebook, Enterprise Mobility, SAP.

[6] Cisco BYOD, Achieving employee Device Freedom & protecting IT networks, August 29, 2013.

[7] SaurabhDeshpande, "Bangalore based startup cashes in on BYODenablement", http://yourstory.com/2014/01/bangalore-byod-simply-office/, 10th January, 2014.

[8] "Cisco BYOD CVD Release 2.2", http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/byoddg.html.

[9] VarunHanan, "The state of BYOD in Corporate India-What's in store for 2014?", http://www.informationweek.in/informationweek/news-analysis/287225/byod-corporate-india-whats-store-2014, January 23, 2014.

[10] http://www.ey.com/GL/en/Services/Advisory/Bring-your-own-device---mobile-security-and-risk.

[11] Pat Fiorenza, "Exploring BYOD in the public sector", http://issuu.com/govloop/docs/byod_government/1?e=3570346/3068763.

[12] http://www.kpmg.com/in/en/issuesandinsights.

[13] ComputerWorld UK Staff, "BYOD-Best practices and effective policies in a bring your own device environment", http://www.computerworlduk.com/business-it-hub/management-briefing/3350113/bring-your-own-device-effective-policies-practice-in-byod-environment/, April 10, 2012.

[14] http://en.wikipedia.org/wiki/Bring_your_own_device

[15] http://www.webopedia.com/TERM/B/BYOD.html

[16] http://www.zdnet.com/topic-byod-and-the-consumerization-of-it/

[17] http://www.trendmicro.com/us/enterprise/challenges/it-consumerization/

[18] http://www.cisco.com/web/solutions/trends/byod_smart_solution/implement.html

[19] Cisco BYOD Smart Solution, Security, Flexibility and Performance for any workplace

[20] http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/byodwp.html

