RESEARCH ARTICLE OPEN ACCESS

Role of Mobile Cloud Applications and Challenges in BYOD

P.Soumya Sree Laxmi[1], K.Kala Bharathi[2],CH.Mary Pushpa[3]

Lecturer(1,2,3), Department of Computer Science, St.Pious X Degree & PG College for Women, Nacharam, Hyderabad,India-5000 076

----------**********----------

Abstract:

Mobile applications brought a tremendous change in today's working environment i.e. stationary work environment is rapidly disappearing. The term mobile computing is very often used for wireless mobile computing - the use of portable devices capable of wireless networking. Mobile computing covers a variety of different hardware and software platforms as well as diverse application. A consumer-led revolution is driving rapid developments in mobile technology. The use of mobile apps is making a line between work and home lives blurring and BYOD (Bring your own device) to work is rapidly becoming a constraint.

Keywords :- **Mobile computing, Mobile Apps, Risk, Security, BYOD.**

----------**********----------

INTRODUCTION:

Business-to-consumer companies embrace smart phones as a medium to reach their customers, more and more of them are creating apps in favor or in addition to mobile web (browser-based) formats. usage of apps and mobile browsers were near equal, with app usage growing at a faster rate than mobile browser use. Mobile Cloud Computing (MCC) is the combination of mobile and wireless networks to bring rich computational resources to mobile users, network operators, as well as cloud computing providers.[1] The challenge for developers is building applications that work across these platforms, since each platform requires different tools and languages.

MOBILE APP TECHNOLOGIES:

Mobile applications and the market scenario have evolved so much in the last decade in the technologies and standards. This directly has impact on the things that one need to decide early in stage in the mobile application development process as how to build and deploy an app.

A. **Native Apps:**Native Apps are built using the development tools and languages that the respective platforms support and so run only on their targeted platforms. End users typically acquire these apps through an online app store. i.e, it is tied to a mobile platform and to the particular mobile device.

B. **Web Applications:** Web applications are nothing but the mobile web portals that are designed, customized and hosted specifically for mobiles. They are accessed through the mobile device's web browser using a URL.

C. **Hybrid Applications:** These are the mobile apps that offer interesting compromise/mix between native and web. A hybrid app is a native app with embedded HTML. Hybrid apps are cross-platform applications that use web technologies (such as HTML, JavaScript and CSS), while still accessing the phone's features.

CHARACTERISTICS OF A GOOD MOBILE APP:

The purchase of applications allowing gaining remote access to company's documents and business processes makes sense only when users will actually be willing to use it. Such application should have the bellow characteristics:

A. ***Simplicity*** **–** One of the biggest advantages of mobile apps is that they save time. Therefore all activities performed on a mobile device should be possible quickly and easily.

B. ***Functionality*** – A good application should primarily do its job. You have to make sure that the solution you buy is capable of handling series of day-to-day tasks that can be performed remotely.

C. ***Security*** **–** Being able to do day-to-day tasks remotely, but at the same time you have to be able to draw a thick line between matters that can be done in and out of office. I think we all agree that business processes and documents crucial to company's interest should be handled only on-premise. Especially when we consider the nature of mobile devices that can be easily lost or stolen.

I. BUILDING BYOD (Bring Your Own Device) :

Presently, enterprises are making use of applications via mobile device; however, the increased focus on digitization is now driving application development for mobile platforms requirements. There is another trend that is important to understand in the context of cloud computing and authentication: the shift in platforms from traditional PCs toward smart phones. In the IT, BYOD, or bring your own device, is a phrase that has become widely adopted to refer to employees who bring their own computing devices – such as smart phones, laptops and PDAs – to the workplace for use and connectivity on the secure corporate network.[3] Enterprise mobility through Bring-Your-Own-Device (BYOD) has been to leakage and loss of customer data and sensitive information. As the organization enables employees to bring their own, the need for using the same devices to access work-related data inevitably presents itself. This presents mainly two security risks:

A. **Malicious apps (malware):** the increase in the number of apps on the device increases the likelihood that some may contain malicious code or security holes.

B. ***App vulnerabilities***: apps developed or deployed by the organization to enable access to corporate data may contain security weaknesses.The below table convey the risk associated with focus on different issues.

Table I

Emerging risks associated with BYOD

Focused Areas	What may happen	New Challenges
User	Users may share their mobile devices containing customer and corporate data with friends and family members.	How to safeguard sensitive data and prevent unauthorized access?
Data	Users may not use their mobile devices for illegitimate purposes or downloading inappropriate/copyright-materials	How to segregate personal and enterprise data?
Device Security	Users may not use and maintain their mobile devices in a secured manner, such as not installing critical updates, routing the devices, downloading illicit apps, etc.	How to control and align security configuration among different devices running on different platforms e.g.,: Android, iOS?
Network	Users may connect to insecure internet access points in public areas such as cafes, airports, shopping malls, etc.	How to mitigate the risk of data loss and leakages through insecure access points in public areas?

II. ADDRESSING GOVERNANCE AND COMPLIANCE ISSUES

A. **Privacy governance:** Increasing privacy legislation is a trend that likely will increase in the near future. As organizations design BYOD security controls, these may interfere with personal expectations of privacy. In order to stay ahead of this concern, organizations are currently addressing privacy concerns in a BYOD policy. A well-formed BYOD policy

should include defined, clear expectations on privacy-impacting procedures.

B. **Monitoring (privacy at work)**: There is a wider variety of laws and requirements around monitoring, wiping and data protection. In order to avoid these privacy pitfalls of monitoring controls, a product should be selected that allows for the ability for monitoring to occur exclusively around work-related mobile activities.

C. **Data protection:** In a BYOD deployment, data protection does not only apply to corporate data. If data is processed by a third party (i.e., if the organization utilizes a cloud email provider), it is important that the data be protected by a data processing agreement with the third party. With the transference of data, the responsibility of protecting that data also should be transferred and compliance verified.

D. **Data ownership and recovery:** "Ownership" should be a key dimension that guides policy settings. As a result, personal and corporate devices will each have different sets of policies for security, privacy and app distribution. The shift from corporate laptop to personal devices has repercussions for data recovery when a device is damaged or lost/stolen. To mitigate unclear responsibilities for data recovery in a BYOD scenario, the organization should have a clear policy stating who owns what data, and whose responsibility it is to maintain backups of data, corporate as well as private.

BENEFITS AND CHALLENGES TO MOBILE APP AND BYOD DEPLOYMENT:

- Customer-focused benefits are also achieved from mobility solution implementation.
- Device security is an issue as new types of mobile devices and operating systems are supported.
- Increased employee responsiveness, decision-making speed, and issue resolution are key benefits.

IV. CONCLUSIONS:

In this paper we have given a brief description about cloud mobile computing and cloud mobile app such as BYOD and comparative to traditional methods, how they are secure and reducing the cost of purchasing the infrastructure and also the benefits of cloud mobile apps in present era by reducing the manpower. By integrating a thoughtful BYOD policy and adopting strategies that are flexible and scalable, organizations will be better equipped to deal with incoming challenges to their security infrastructure posed by the use of employees' own devices. The introduction of appropriate policies will help organizations to become smarter and make their employees more aware of the challenges by the use of personal devices.

ACKNOWLEDGMENT

We are thankful to the Principal and the management St.Pious X Degree & PG College for Women, for encouraging publications work. We are grateful to the HOD and our colleagues for the support rendered in completing this paper.

REFERENCES

[1] Fangming Liu, Peng Shu, Hai Jin, Linjie Ding, Jie Yu, Di Niu, Bo Li, "Gearing Resource- Poor Mobile Devices with Powerful Clouds: Architecture,Challenges and Application";,IEEE Wireless Communications Magazine, Special Issue on Mobile Cloud Computing, vol. 20, no. 3, pp.14-22, June, 2013.

[2]I. Kelenyi et al., "CloudTorrent — Energy-Efficient BitTorrent Content Sharing for Mobile Devices via Cloud Services," Proc. IEEE CCNC, 2010.

[3] http://www.webopedia.com/TERM/M/mobile-device-security.html