**INTRODUCTION .......................................................................................................................................................**

**WHY IS SYNE- MOBILE NEEDED? ...................................................................................................................................**

 Problem 1:

 *Problem 2:*

 Problem 3:

 Problem 4:

**BUSINESS OPPORTUNITY .........................................................................................................................................**

**CHALLENGES FACED BY SYNE- MOBILE .........................................................................................................................**

**TOPIC OF THIS PAPER AND ITS SCOPE ......................................................................................................................**

**SOLUTION OFFERING BY SYNECHRON ......................................................................................................................**

 *Syne-Mobile – High-Level Architecture .............................................................................................*

**ABOUT SYNE-MOBILE ..................................................................................................................................................**

 *Module 1:*

 Module 2:

 Module 3:

 Module 4:

**CASE STUDY ...........................................................................................................................................................**

 *Context ..........................................................................................................................................................*

 *Objectives......................................................................................................................................................*

 *Solution .........................................................................................................................................................*

 *Salient Features ............................................................................................................................................*

 *Conclusion .....................................................................................................................................................*

**ABOUT SYNECHRON ..............................................................................................................................................**

**ABOUT THE AUTHORS ............................................................................................................................................**

**INTRODUCTION**

Through Synechron’s relationships with leading customers around the world, it was noticed that increasingly, wireless carriers and subscribers were demonstrating a growing demand for security of their mobile devices i.e. to protect not only their phones, but also the valuable data and content on the phones. (along with a strong technical support)

Today, business is increasingly likely to be a mobile enterprise, conducted using devices that might not have been existed a few years ago.

Nowadays, business is growing dynamically as a digital enterprise and almost every industry conduct their operations using devices that were non-existent few years ago. has seen a tremendous rise

Mobile devices also add significant value to people and organizations through increased efficiency and productivity. The world around us is also digitally transforming in a way that is having significant impact on how people and enterprises operate and this is affecting the technology and systems that are designed and built to support them.

However, this era of mobility introduces new risks to the data. SyneMobile enables secure mobility by providing comprehensive risk management across Android devices to protect against app, network, and device-based threats while providing visibility and control over data leakage.

**Existing Problems/Limitations**

**Secure Data Backup with interminable growth and lengthening retention periods**

A expanding base of mobile users with an ever-expanding spectrum of devices to access, store, and share data has created more complex data storage environments.

A growing number of mobile subscribers with an unbounded and broad range of devices to save, protect and access data has developed more complicated data storage systems.

This makes it one of the most important assets for mobile users and should be protected without any failure.

The challenges of protecting and storing expanding volumes of users' data can leave any organization overwhelmed and looking for alternatives to provide a comprehensive and quintessential cloud data backup solution that spans both centralized data (on servers) and distributed data (on mobile devices, on laptops and PCs).

The challenges of securing and saving inflated amount of customers data can make any enterprise look for solutions that can provide a comprehensive and quintessential cloud data backup program which is capable of managing extensive data distributed across various platforms.

**Solution -**

SyneMobile offers a potential solution for this and allows data(photos, videos and contacts) to be stored and accessed in the most secure manner which uses a highly compressed, encrypted stream to ensure data confidentiality without sacrificing performance. It also offers a scalable and centralized management system, leveraging a very simple and automated scheme that is attractive to the customers.

**Effective and Instant Mobile Technical Support**

In this age of customer oriented industry, providing technical support has become an integral part of any business or service oriented organization. Technicians are employed to solve problems or a deceptively complex task. Any particular encounter involves multiple layers of non-linear problem solving, or scenarios that are rarely explored or considered. It might be a case where the problem statement/scenario doesn't even exist or may be incorrect and complying with these kind of requirements do not help resolving the customer problem but often end up intruding into that task.

**Solution -**

There is a huge void which needs to be fill in to keep the customers/users engaged with the business. This can be achieved by -

* Determining what steps to take, in what order, on what device given a very wide range of settings.
* Relying on someone with strong technical background with a complete know how and who can perform right actions.

The application provides a mechanism which allows the tech agents to perform these actions by enabling them to access user's device remotely and operate on it. Agents can navigate through the settings menu or they can also draw on the device screen and guide the users to solve and fix the issues faced. This not only makes sure that the problem is resolved but also saves a lot of time users spent on interacting with the customer agents.

**Threats to Mobile Security**

Security and privacy are the two highly dynamic and fast- paced challenges faced by end users and since mobile phones become user programmable i.e. they supports app downloads, the scope for device protection extends and is not limited to data-theft. There is also a possibility that a virus-infected or malware app be installed on the device and may not only harm the device OS but can also act in leakage of user data. Mobile apps are particularly susceptible to reverse-engineering attacks that expose the code and app logic, allowing malicious entities to identify and exploit vulnerabilities.

Threats can be categorized as-

Application-level:

Major threat which falls in this category is malware and side loaded apps, these apps are commonly repackaged and also distributed through third party app stores. Sometimes users also go for processes like jail-breaking or rooting which exposes their mobile devices and makes OS security features ineffective. This makes it easy for the malware apps to break in and get privileged access to the resources on the device.

Data or Storage-Level:

These threats are related to files which we copy or transfer to the device, these can be text documents, or may be an apk(android package) file. Sometimes these are virus infected and can vitiate the whole storage system.

Web-Level:

These kind of threats do not directly impact devices but still the users' privacy is at risk from these kind of threats. One of the main web related threat is phishing, which uses emails and other un-trusted platforms to send across links to a phishing website which is developed to trick the users into providing sensitive information like his credentials.

**Solution -**

After speculating all the threats that can exploit a device and make them vulnerable to attacks, along with the limitations of the OS, it becomes imperative to build an application with in-built security controls and also equipped with self-defense mechanisms. SyneMobile implements all this and offers a multilayer protection including:

* Antivirus protection.
* Detecting phishing and malware websites and alerts the user if they are trying to access it on mobile web browser.
* Real-time protection, including intrusion prevention and alerts that an attack/threat is in progress.

**Effective Telemetry and Big Data Analysis:**

The day a user purchase a mobile phone, the device starts collecting and storing data. Over the course of time, user starts interacting with various applications and keep on performing various tasks multiple times. This creates a pattern which the user is not aware of but can be used to conclude the behavior of the installed apps and can also tell you the health of the device. The major challenge faced is to determine upfront which data is relevant and the variety and volume of the data hence gathered should be utilized to provide accurate and timely decision making benefiting the end user.

**Solution -**

Telemetry implementation is an updated approach to the transition of mobile applications and is the need of the day. Based on a deep understanding of the telemetry options and careful data analysis, we have developed a telemetry architecture which enables SyneMobile to process information around user metrics, application data, crash reports and a lot of other statistics about the device. It also gives the ability to query big data and generate insights(from large scale users data) which is delivered to them via proper channels like notifications.

**Use-case:**

To better understand this, let us consider a scenario where a user is running on low storage and how SyneMobile generate insights based on this data-

**Decision Logic:**

* Is the free space less than X% of the overall device storage?
* Has the user received a notification about low storage recently?

**Recommendations:**

* Uninstall applications that are not in a frequent use.
* Remove unwanted photos/videos.

The data is used to generate rich HTML content and delivered to the user.

**About SyneMobile -**

The SyneMobile application framework is an all-in-one protection application and companion web portal featuring Security, Recovery, Content Backup, Health Scan, and advanced support functions such as Telemetry analysis and technical support including remote access with live chat.

SyneMobile will be available across all Android devices, and the web portal will be accessible through all major browsers including optimization for mobile browsers.

The overall product initiative is to create a compelling “shrink wrap” Protection Application (PA) product which is integrated with Device Protection (DP) and Advance Technical Support (ATS) in order to provide a complete Mobile Solution (MS) offer.

**Objective**

Protection applications objective is to provide data management features such as backup and restore contact and content data; recovery options such as locate, lock, wipe, and alarm; security options such as antivirus, app assist, and malware detection; and mobile technical support services. AMA applications enhance mobile experience and satisfaction for subscribers, and provide value-added services for carriers, OEMs, and partners.

User's data is the most sensitive and needs to be secured at any cost.

In order to achieve these objectives the product is developed as a complete mobile solution consisting of following key components:

**Data Backup -**

The application provides a backup system which is smart enough to back up only data that has not already been backed up. There is a complete algorithm which makes sure to cross-check the number and type of files on the cloud and on the device, along with the storage space, network restrictions, OS settings and other user defined configurations before initiating a backup. Apart from these stringent configurations, the application makes sure that the data transfer occurs in a secure manner and offers enhanced security options including data encryption where key management is with the client.

It includes the following features:

* Backup - Backs up and restores contacts on mobile devices automatically.
* Sync - Synchronizes automatically or manually from device to website and vice versa
* Manage - Provides server side management for contacts, such as add, edit, and import.

**Device Protection & Security -**

The application enables secure mobility by providing risk management across Android devices to protect against network, app and device based vulnerabilities while providing visibility and control over data breach. It includes a comprehensive suite which enables the user to leverage its capability to provide security against malware, viruses, phishing sites, Trojans, etc. It also has a feature which warns the users against a possible phishing or malware website if they are visiting any URL on the device browser.

The app is powerful enough to detect threats and risks, such as:

* Malware and Trojans that can extract data from the device.
* Side-loaded app behaviors that pose threats.
* Man-in-middle attacks.
* Jailbreak or deleterious root.

**Device Recovery-**

Recovering a device is another integral aspect for a complete mobile solution as it enables the users to have full control of their device even if it's not with them(in case of theft or misplaced). This functionality consists of the following features:

* Locate - Locates a missing phone with GPS.
* Alarm - Sounds an alarm to find a misplaced phone, even if it's on silent or vibrate.
* Lock - Remotely locks a missing phone to prevent unauthorized use.
* Wipe - Remotely erases contacts from a missing phone to secure your privacy.

**Device Health Monitoring -**

One of the most important thing which always keeps a user engaged to an application is the way it lets you know how healthy your device is. SyneMobile enables the user to scan through the apps and data storage to gather information and run a complex algorithm to conclude the device and battery performance which might be helpful in identifying and resolving battery related issues. It also indicates the user about the apps which are running high on memory, ones who use a lot of storage space and also about the ones who consumes a lot of battery.

**Know It All(KIA) -**

KIA is a knowledge based value-add feature which enables SyneMobile users to get tips and other articles with relevant information they might be seeking about their device or it may be related to any technical issue they are facing with their mobile phones. They can also perform a search for anything related to their device, ranging from security settings to Bluetooth or Wi-Fi connection issues and if available a content-rich article will be provided to them containing step-by-step details.

The added advantage of this feature is that it will gather the data across its user base, and with a complex algorithm, it will generate articles/tips which will be a combination of device make and model, OS version and will provide them to specific users only. So, for example, a user having a mobile with a particular make, model and OS version will receive articles/tips which will be specific to that device only.

**Advanced Technical Support with Live Chat-**

SyneMobile provides flexibility to the users to opt for instant tech support or go for live chat depending on the urgency and complexity of the issues they are facing. They can chat with care agents and communicate the problems they are struggling with or they can contact tech agents who can remotely access their devices and resolve the issues.

**Telemetry and Data Anaylsis -**

Mobile device telemetry data is a main information source for personalized engagement and it measures the real-time user experience. We then use unique, big data analytics to associate the anonymized device data with customer context to enable personalized engagement that is timely, relevant, and actionable for the user.

This is how the data is collected(high-level) and sent across the servers -

Telemetry data is uploaded from the device to the Asurion cloud-based analytics system. Collection

and transmission of device telemetry are optimized to balance frequency of collection for obtaining

up-to-date information with minimizing battery drain and data volume. We practice the following

key tenets of collection and optimization:

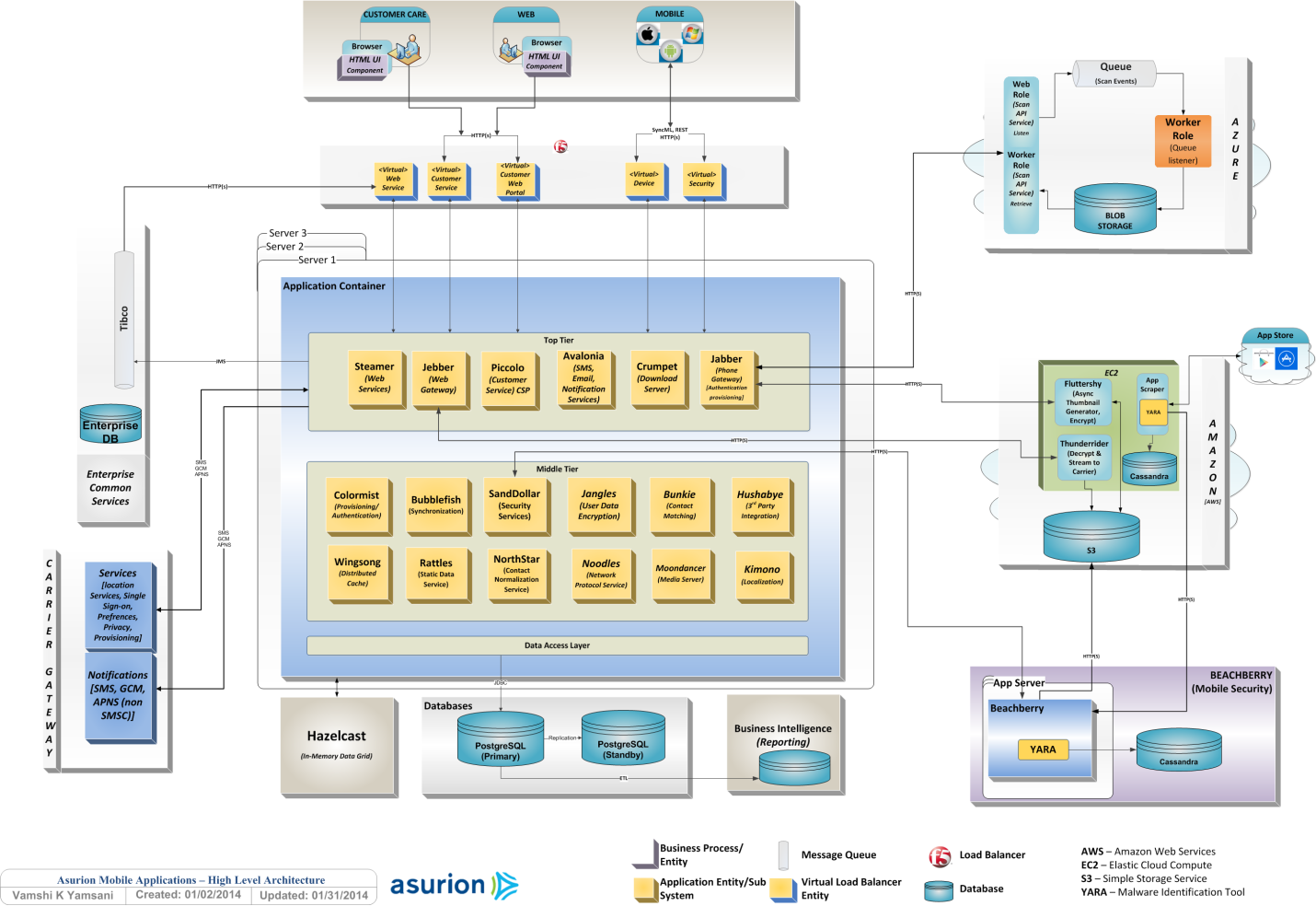
* Personally Identifiable Information (PII) is not collected from the device and device identity is anonymized.
* All data is compressed on the device to minimize data transmission costs.
* The device can be configured to send data only when connected to Wi-Fi or only when the device is charging.
* Payloads are as small as possible

A User can also configure the settings on how he/she want to send this data or if he wish to switch it off, he/she can also do that. These are the properties that can be configured:

* Whether the report is generated.
* Frequency of transmitting the report.
* Maximum size of the report, in bytes.
* Maximum number of reports to store.

**Architecture:**

**High Level-**

****

**Components-**

Application Layer

Amazon Cloud

Database Storage

Hazelcast

**Enterprise Data Services-** SyneMobile can be easily integrated with any Enterprise DB or other 3rd party entity to provide Authentication and Validation services. Users' personal details will never be stored on our app server enabling a secure layer for those organizations which are stringent on data breach of their customers.

Web Application Container

**Mobile Security Engine-** This component specially designed for indentifying threats and other malwares and keep records for the same. It communicates with the MT security services and provides a protection layer for the application.

Business Intelligence(Reporting Tool)

**Telemetry-**

**KIA-**

**Mobile Technical Support-**

**Case Study**