International Journal of Advanced Engineering & Innovative Technology (IJAEIT)
Volume 1, Issue 4, October -2014

ISRA IMPACT FACTOR: 0.42

Mitter – Bitter Monitoring System Using Security Profile

Deshpande Komal N. , Gade Reshma S. , Dighe Sonali D. , Ekshinge Archana P.

Abstract: Now days the use of Smartphone is highly increased in the business. The Smartphone having their own storage capacity gives the users platform to do various operations and update while the user is moving from one location to another so, it needs the security. In this paper we are giving security profile to user. This is the monitoring system for the employee. It is the application which provides facility to the manager to monitor the employee's office Smartphone. The manager can track the employee day to day activities such as incoming call, outgoing call, message history, web history, data usage and the system can track the location of employee. All this data is stored into the centralized server manager have the access of the centralized server can view the employees Smartphone activity. With this system the organization can monitor the employees Smartphone activity and can keep away the wrong things happen such as data leakage and the misuse of the office Smartphone.

Keywords: Security profile, GPS, Tracking, Android, Monitoring.

INTRODUCTION

Smartphone's provides the facility to perform several tasks while being on the move. The end users want their personal Smartphone's connected for their work IT infrastructure. Companies also provide mobile versions of their desktop applications. The Smartphone's expands employee's productivity. A huge number of companies are even using the BYOD: Bring Your Own Device policy, using the Smartphone to provide mobile access to company's applications. Now day's also the companies provides the Smartphone's with two Subscriber Identification Module. With these various security issues may arise. The Smartphone carries company confidential data. Employee Tracking System using the Smartphone is supported by business Organization. Employee tracking system accept Smartphone network, the system gives a new generation Employee monitoring system. The system has the requirements. Easy to implementation and can easily add functions, ability to manage number of employee conveniently, flexible for mobility of employee who is working in concern. For these requirements, we proposed new generation employee tracking system uses 3G communication technology between Smartphone's, and trace employee information using Global positioning system. The employee tracking system contains the telephony manager for determine the information of the employee. Android Smartphone's which each employee holds, and the central server which stores employee tracking information. The employees tracking information in this system holds the position and time information of android Smartphone. Whenever the employee crosses particular restricted area an alert message will be sent to the manager's Smartphone. Using this system it possible for the manager of an organization to trace the location of the particular employee. The android has several features and them mainly focuses on application framework enabling reuse and restoration of components.

Deshpande Komal N. , Gade Reshma S. , Dighe Sonali D. , Ekshinge Archana P. Research Scholar at Department of Computer Engineering ,Navsahyadri Education Society's Group of Institutions, University of Pune, Naigaon, Pune 412213 India

EXISTING SYSTEM

In the existing system employee location tracing is done by fixing tags in various location for identifying the current exact position of an employee. The android terminal is attached to Bluetooth and wireless LAN. Tracing is made to shorter distance while using Bluetooth. Because the Bluetooth has very short bandwidth. The tracing system is not secure when compared to the advanced system. The communication link to the central server is managed by wireless LAN which is relatively slow when compared to the 3G network. The dynamic paring of mobile Smartphone is mandatory. The network is more complicated and it is unreliable. The message is transported through wireless LAN and it is not secure.

A. Drawbacks of Existing System

The Managers cannot trace out the Employee's activities in the mobile, like SMS and Calls Web history, data

usage. The Managers cannot know the Employee's exact location or position.
There is a possibility of data loss during the message transfer from one terminal to another terminal. There is a failure in data transfer due to 2G network. The existing system is only useful in particular organisation or company.

B. The Features of the Proposed System
The Manager can easily track the Employee's day to day activities like SMS, MMS, call history, web history; data the manager can trace the position of the employee at anytime. It is possible to trace the exact current position of the employee with the help of GPS

SYSTEM ARCHITECTURE

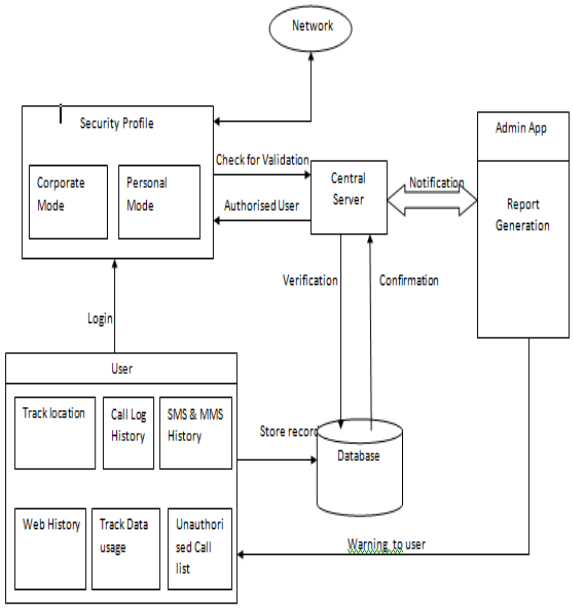

Fig 1: Architecture of proposed system

ALGORITHM

AES algorithm:
The system mainly focuses on protecting the data from some unauthorised users who could leak some generalized information about the employee and the organization. It is essential to implement the fundamental objectives and goals of information security, such as confidentiality, integrity, authentication, and anonymity typically using this encryption algorithm. Encryption is the process of converting a plaintext message into cipher text. The cipher text can be decoded again into the original message and get the plain text again. An encryption algorithm with a key is used in the encryption and decryption of data.
Like DES, AES is a symmetric block cipher. This means that it uses the same key for both encryption and decryption. However, AES is quite different from DES in a number of ways. The algorithm Rijndael allows for a variety of block and key sizes and not just the 64 and 56 bits of DES' block and key size. The block and key can in fact be chosen independently from 128, 160, 192, 224, 256 bits and need not be the same. However, the AES standard states that the algorithm can only accept a block size of 128 bits and a choice of three keys - 128, 192, 256 bits. Depending on which version is used, the name of the standard is modified to AES-128, AES-192 or AES-256 respectively. As well as these differences AES differs from DES in that it is not a feistel structure. Recall that in a feistel structure, half of the data block is used to modify the other half of the data block and then the halves are swapped. In this case the entire data block is processed in parallel during each round using substitutions and permutations.
A number of AES parameters depend on the key length. For example, if the key size used is 128 then the number of rounds is 10 whereas it is 12 and 14 for 192 and 256 bits respectively. At present the most common key size likely to be used is the
128 bit key. This description of the AES algorithm therefore describes this particular implementation.
Related characteristics is given:
• Resistance against all known attacks.
• Speed and code compactness on a wide range of platforms.
• Design Simplicity.

Workings of a Round

The algorithm begins with an **Add round key** stage followed by 9 rounds of four stages and a tenth round of three stages. This applies for both encryption and decryption with the exception that each stage of a round the decryption algorithm is the inverse of its counterpart in the encryption algorithm. The four stages are as follows:
1. Substitute bytes
2. Shift rows
3. Mix Columns
4. Add Round Key

The tenth round simply leaves out the Mix Columns stage. The first nine rounds of the decryption algorithm consist of the following:
1. Inverse Shift rows
2. Inverse Substitute bytes
3. Inverse Add Round Key
4. Inverse Mix Columns

Again, the tenth round simply leaves out the Inverse Mix Columns stage.

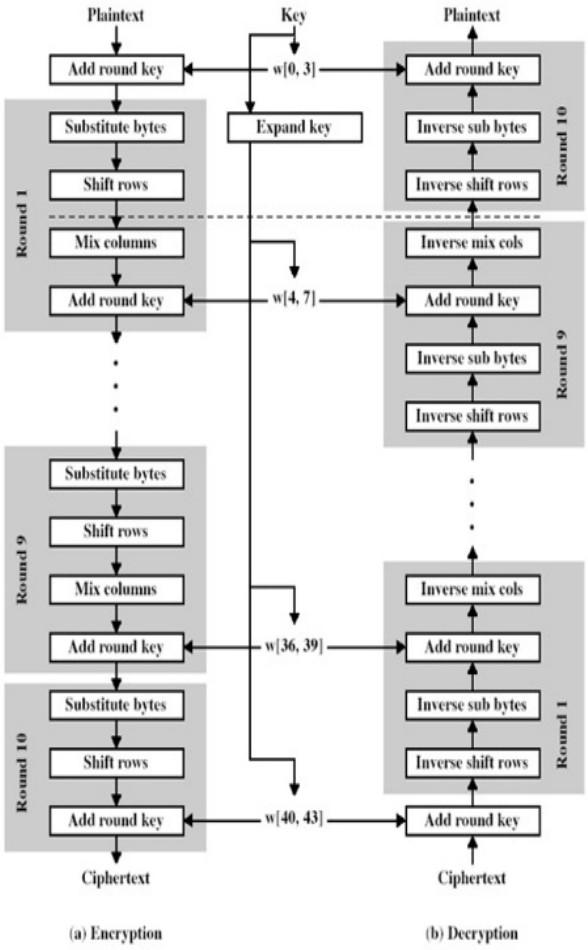

Figure: 1 Overall structure of the AES algorithm.

CONCLUSION

In our paper, we have described Apex {an extension to the Android permission framework. Apex allows users to specify detailed runtime constraints to restrict the use of sensitive resources by applications. The android framework achieves this with a minimal trade of between security and performance of the system. The user can specify his/her constraints with the help of simple interface of the extended Android installer called Poly.
The extensions are incorporated in the Android framework with a minimal change in the code base and the user interface of existing security architecture.
Every Android users need as a way to determine if applications are leaking their personal information or not. To this end we are going to present Android Leaks, as a static analysis tools for ending potential privacy leaks in Android applications. In order to make Android Leaks, we have created a mapping between API calls and the permissions they requires.

FUTURE WORK

In Our System, Employees should not use their company phone for personal use, if they call to an unapproved number from employee list; it will be logged on to server. Calls Logs should show the details of incoming and outgoing calls history from employee's phone like date, time, and phone number. Manager should get the message history from employee cell phone like text messages (inbox/sent/draft) and multimedia message with date and time. Employee location gets by using the GPS. If employee goes outside of approved geographical zones then a notification is sent to managers. Managers should be able to update list of unauthorized websites that should not be accessed by employee. Managers can dis-approve the international calls for the employee. No of unapproved calls, exceeding data usage is calculated for each employee then k-means clustering algorithm is applied on these parameters to calculate the mean and different clusters. Each cluster indicate a different employee behaviour (Good-Loyal/Average/Bad)

REFERENCES

[1] William Enck, Machigar Ongtang, and Patrick McDaniel. On lightweight mobile phone application cortication. In CCS '09: Proceedings of the 16th ACM conference on Computer and communications security, pages 235{245, New York, NY, USA, 2009. ACM.

[2] Adam P. Fuchs, Avik Chaudhuri, and Je_rey S. Foster.SCanDroid: Automated Security Certi_cation of Android Applications. In Submitted to IEEE S&P'10: Proceedings of the 31st IEEE Symposium on Security and Privacy, 2010.

[3] Google. Android Home Page, 2009. Available at: http://www.android.com.

[4] Google. Android Reference: Intent, 2009. Available at: http://developer.android.com/reference/android/content/Intent.html.

[5] Google. Android Reference: Manifest File - Permissions, 2009. Available at: http://developer.android.com/guide/topics/manifest/manifest-intro.html\#perms.

[6] Google. Android Reference: Security and Permissions, 2009. Available at: http://developer.android.com/guide/topics/security/security.html.