International Journal for Multidisciplinary Research (IJFMR)
ISSN: 2582 – 2160, Volume - 1, Issue - 2

RAKSHAK: AN IOT BASED INTRUSION DETECTOR

[1]Krishan Kumar, [2]Amandeep

[1, 2]Assistant Professor
[1, 2]Department of computer science and Engineering
[1, 2] Guru Jambheshwar University of Science & Technology, Hisar,India

***Abstract*- 'Rakshak' is an IOT based android application which informs the owner of the area where it established. It is a platform thatcapturesan image through camera record Voice by speaker and records all the unusual intrusion and misshaping where it setup. This framework deployed to collect information from the house, office and geographical area where the userwants surveillance. It sensing all unusual activity through the sensor and information via SMS or Signal application approach to the user. It helps to catch the culprit. This application can be installed where the userwants safety and avoid inconvenience in his life.**

***IndexTerms:* -Android, Intrusion, SMS, Motion, Camera, Sensors etc.**

I. INTRODUCTION

Nowadays every city newspaper is full of theft, dacoity, robbery, spying incidents. Means protection is the main matter of concern in today's lifestyle. Every household has valuable items at their home such as documents, jewelry, antiques etc. And in the absence of housemates,anyone can enter the house and can do intrusions [1]. Here the house may lose every expensive thing and no one can identify who has done so and also when it happens those housemate's remains unaware. With the help of this intrusion detection app, immediate actions can be taken. So it will help in reducing the prosecution cost of police, Govt. etc. As voice samples are also good evidence ofa crime so intrusion app will record the conversation of the intruders. This app will be switch enabled. So, we need a system which can spy on the intrusion. Hence, we think of using our old android enabled mobile phone to be used as an intrusion detection system with the help of an Android-based intrusion detection spying App [12].

Advantages of RAKSHAK

RAKSHAK is for people who want to keep an eye out for intrusions into their home, office, hotel room or other private space [6].

- RAKSHAK turns an extra phone into a motion, sound, vibration, and light detector, watching for unexpected guests and unwanted intruders.
- RAKHAK notifies about intrusion event instantly and access the logs remotely or in-person later [6].
- RAKSHAK immediately informs the housemates about the intrusion via text message or internet too.
- RAKSHAK detects every activity of the intruder on the premises and it will also click snaps after sensing unusual things.
- RAKSHAK makes use of phone sensors such as a proximity sensor, light sensor, vibrator, and camera.
- RAKSHAK helps the police in catching the theft by fetching the data from the app. Data like their voice, their snaps, etc.

Methodology and Technologies use to Develop

There are different technologies are used:

- Java JDK5 or later version [3].
- Android Studio [4][5].
- SDK [6].

Android &SDK

Android is a mobile operating system developed by Google, based on the Linux kernel and designed primarily for touchscreen mobile devices such as smartphones and tablets [5][20].

A software development kit (SDK or "devkit") is typically a set of software development tools that allow the creation of applications for a certain software package, software framework, hardware platform, computer system, video game console, operating system, or similar development platform [6].

Java & JDK

Java is a general-purpose computer programming language that is concurrent, class-based, object-oriented, and specifically designed to have as few implementation dependencies as possible[4][5]. It is intended to let application developers "write once, run

anywhere" (WORA), meaning that compiled Java code can run on all platforms that support Java without the need for recompilation. Java applications are typically compiled to bytecode that can run on any Java virtual machine [22] [3].

Related Work (Present System)

Presently, the intrusion can be detected by many systems like CCTV with recording, infrared security system etc. This system records the video, records the sound, and they even alert by switching alarm [10].
But these systems are vulnerable because:

- Their data can be cleared after the action of intrusion by the culprits without any authentication.
- These systems/devices can be damaged.
- If their electrical connectivity is lost they will stop working.
- They are unable to inform the owner immediately by SMS or signal app.
- These systems are expensive.
- The data cannot be fetched online from anywhere.
- They cannot work as a spy.

Modules &Proposed Work

Advantages of the Proposed System

- The system will work as a spy.
- This system is not as expensive as the user can use any old any android enables mobile phone.
- Using this system, the detected events can be fetched online from anywhere.
- The system will continue its work even without electricity as it contains a battery.
- The remote access system is protected by a password. So, a valid user can access the data.
- During an unusual event, it will instantly inform the owner via SMS.
- The data cannot be cleared as the data is sent to the owner just after the detection over the internet.

Modules

The Entire Application is mainly categorized into three main phases or views three dashboards are created for the different kind of activities it includes [9].

1. Home screen dashboard.
2. Logs
3. Manual setting

Home Screen Dashboard

Home screen dashboard is the first screen which opens on starting the application. There a timer is given which help to set the duration after which you want to activate the app. The can be changed and the START NOW button is triggered. On this dashboard Camera, microphone setting buttons shortcuts are also available.

Logs

Logs as its name suggest that log means the intrusions which are detected by the app are found here. The logs are found according to the number of activations. And a number of intrusion or events detected are in one logonone-time activation. The logs will be shown with the date and time of detection of an event [14].
There is also a yellow color play button which will navigate you to the home screen dashboard.

Manual Setting

Here every minor configuration is done. Like the phone number on which the user wants to receive message is inserted in setting dashboard. The sensitivity level of the camera, vibrator,and microphone is to be set from here. The notification duration is also altered from here. The setting of video i.e. whether we Want the app to record the intrusion video or not is being set from here. Remote access can be controlled from this dashboard [5].

Submodules

Sensors

Here we will set the sensitivity level of every used sensor [16] [17]. Like how much intensity of sound it will detect as an event, how much intensity of light it will detect, what speed of movement it will record etc. these works are done by

Camera Sensitivity option

Sound Sensitivity Option

Movement Sensitivity Option

Select Camera option is also there. It will help the user to choose one camera out of the two like front Camera or the back Camera.

Notification

Rakshak app uses two kinds of notification system one using SMS and the other is uses another App named "Signal App". For both, we should have an active mobile number and should have an account on Signal App. In notification module, you can set the preference for the notification that where you want to receive the notification on SMS or on Signal App. For Signal App you need a verification code which is received from the Signal network. And for SMS user need to save the number on which he wants to receive the intrusion notification.Now on how much time you need the notification can also be fixed from this module.

Remote Access

To remotely access the data captured by the app we a feature provided in the remote access module.

The Rakshak app uses tor browser to remotely Access the data. In this module, a switch is given to give permission for remote access. The service address is provided by them tothe robot. We can also set a remote password to make the remote access more secure.

Video Setting

The module for setting the switch for video recording and to set the length of the video to be recorded on intrusion.

Context Diagram of RAKSHAK

The context Diagram the system's interactions with the outside world are modules purely in terms of data flows across the system boundary. The context diagram shows the entire system as a single process and gives no clues as to its internal organization [21].

Fig 1: context diagram of RAKSHAK

This DFD shows all the processes together with all the intrusion activities sensed by phone. It shows the true flow i.e. how data is actually flowing in the system. Data is coming from which table and going into which is clearly shown by this DFD. This DFD is the main reference for the development of the system. After understanding the whole system, the application developer will fall back upon this DFD during the development phase [18].

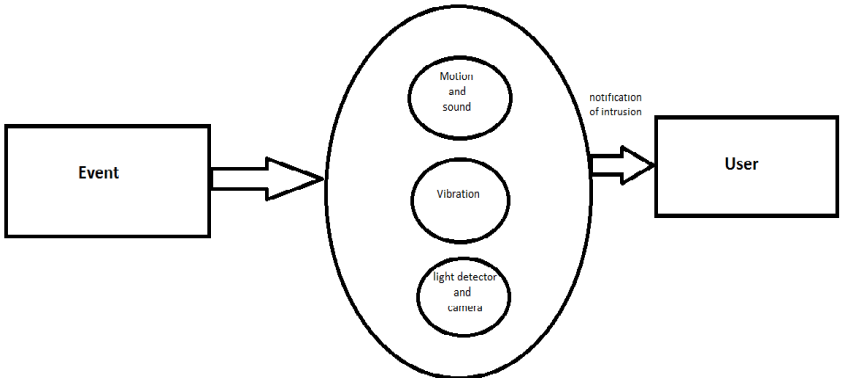

Fig 2. Proposed data flow diagram

CONCLUSION

Now a day's crimes are increasing day by day. And hence the number of the case are increasing in the courts are increasing day by day. Lack of evidence provides dates and dates in the court and due to lack of evidence the culprit is left free. So as to put every sensitive, valuable thing under surveillance and informs the owner immediately about the intrusion so that he can try once to catch the thief red-handed. Or if not able to catch he can inform the police instantly after the intrusion and can provide photos, voice sample to the police.

Future Enhancement

Without a doubt, the project undertaken can be extended to a variety of surveillance apps in the future. Some potential ideas are:

- Multiple mobile numbers can be added to receive the SMS about intrusion such as the mobile number of Police, mobile number of a security guard of the society.
- In future, this app can be linked to a system which can lock the house, office from outside so that the intruder can be caught locked inside the house.

REFERENCES

[1] https://en.wikipedia.org/wiki/Intrusion_detection_system

[2] https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-detection-system-ids.

[3] http://www.oracle.com/technetwork/java/javase/downloads/index.html.

[4] https://developer.android.com/studio.

[5] https://en.wikipedia.org/wiki/Android_Studio.

[6] https://en.wikipedia.org/wiki/Software_development_kit.

[7] Dr. S.Vijayarani1 and Ms. Maria Sylviaa.S "INTRUSION DETECTION SYSTEM – A STUDY", International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 4, No 1, pp. 31-44, February 2015.

[8] Peyman Kabiri and Ali A. Ghorbani, "Research on Intrusion Detection and Response: A Survey", International Journal of Network Security, Vol.1, No.2, PP.84–102, Sep. 2005.

[9] Unspam; LLC a Chicago-based anti-spam company. "Website for the project honeypot," http://www.projecthoneypot.org/.

[10] M. Analoui, A. Mirzaei, and P. Kabiri, "Intrusion detection using multivariate analysis of variance algorithm," in Third International Conference on Systems, Signals & Devices SSD05, vol. 3, Sousse, Tunisia, Mar. 2005. IEEE.

[11] A. Zhong and C. F. Jia, "Study on the applications of hidden Markov models to computer intrusion detection," in Proceedings of Fifth World Congress on Intelligent Control and Automation WCICA, vol. 5, pp. 4352–4356. IEEE, June 2004.

[12] D. Barbara, J. Couto, S. Jajodia, and N. Wu, "Special section on data mining for intrusion detection and threat analysis: Adam: a testbed for exploring the use of data mining in intrusion detection," ACM SIGMOD Record, vol. 30, pp. 15–24, Dec. 2001.

[13] D. Barbara, N. Wu, and S. Jajodia, "Detecting novel network intrusions using Bayes estimators," in Proceedings of the First SIAM International Conference on Data Mining (SDM 2001), Chicago, USA, Apr. 2001.

[14] M. Bilodeau and D. Brenner, Theory of multivariate statistics. Springer - Verlag: New York, 1999. Electronic edition at ebrary, Inc.

[15] M. Botha and R. von Solms, "Utilising fuzzy logic and trend analysis for eff ective intrusion detection," Computers & Security, vol. 22, no. 5, pp. 423–434, 2003.

[16] Susan M. Bridges and M. Vaughn Rayford, "Fuzzy data mining and genetic algorithms applied to intrusion detection," in Proceedings of the Twenty-third National Information Systems Security Conference. National Institute of Standards and Technology, Oct. 2000.

[17] D. Bulatovic and D. Vitasovic, "A distributed intrusion detection system based on Bayesian alarm networks," Lecture Notes in Computer Science (Secure Networking CQRE (Secure) 1999), vol. 1740, pp. 219–228, 1999.

[18] https://en.wikipedia.org/wiki/Data_flow_diagram.

[19] https://play.google.com/store.

[20] http://cybercinatics.com.

[21] http://isanalisti.net.clearwebstats.com.

[22] http://www.acornsoftware.net.