Smart Lost Gadget Recovery System Using Cloud and Mobile Technologies

Mrs. B. Kala[1], R. Harshini[2], M. Deepika[3], K. Harini[4], M. Harini[5]

[1]Assistant professor Department of Computer Science and Engineering,
V.S.B Engineering College, Karur, Tamil Nadu
[2,3,4,5]Department of Computer Science and Engineering,
V.S.B Engineering College, Karur, Tamil Nadu

Abstract

Electronic devices such as smartphones and laptops are often lost in public locations, which creates a monetary expense and security risks for the data on those devices. The retrieval methods and retrieval process already in place are generally time-consuming and conducted through manual means. The Smart Lost Gadget Recovery System (SLGR) has been developed to provide the user with a secure, organized, and digital platform for addressing this same issue. SLGR uses cloud storage, a mobile application, and unique identifiers, such as IMEI, Serial Number, and MAC Address, to allow users to both register their devices as well as report a lost device, and allow appropriate users to attempt a match and reporting of a device found. Lost devices could be matched by text only or by image as well, just for being able to match missing gadgets more quickly. The device owner is notified through the mobile application when a match is found. SLGR theoretically creates a more quick and reliable means of device recovery than is currently in place. This paper will explore the design, methods, and technologies used for SLGR implementation. Additionally, applications, disadvantages, reflections, and future developments will be evaluated as well.

1. Introduction

In our current digital age, devices such as smartphones, computers, and tablets have ultimately become an integral aspect of life for humans. Devices used to only have communication and entertainment purposes, but now devices also serve as a storage space for pertinent personal information and digital content related to work. Common life activities like banking online, school, business communication or health monitoring all typically engage with these electronic devices, enhancing the significance of their impact. As a result, losing or stealing an electronic device not only leads to a financial risk, but also creates a data security risk if the data is however sensitive (i.e., identity theft, privacy breach, unauthorized access to sensitive data).

Traditional methods of recovering gadgets tend to be mostly manual and inefficient. Some telecommunication providers provide tracking capabilities based on International Mobile Equipment Identity (IMEI) numbers, but again, this is only possible if a user works with government or law enforcement agencies, which may not be accessible to every user. Other device-specific approaches, like Google’s “Find My Device” or the built-in Apple “iCloud” method can track devices as well, but again, limited to a brand ecosystem and usually required to be “on.”” The discontinuity between these processes provides a good platform on which an meta-use, secure and scalable gadget recovery system can be built.

There are several advantages of the new system. First, it creates a global digital registry of devices, which can be verified anywhere that there is cloud storage. Also with mobile application solutions, the system provides user-friendly interface by the gadget owner and finder that heightens participation and reporting. Lastly, the platform will have verification security, which will be One-Time Passwords (OTP), and an encrypted database that enhances confidence to the platform.

A. Contributions of this Work

The main points of this paper can be summarized in the following way:

- An ecosystem and brand-agnostic recovery system.
- Unique identifiers (IMEI, MAC ID, serial number) to be incorporated with image-based verification to obtain a higher matching accuracy.
- A cloud enabled architecture that will provide scalability and accessibility at a global level..

B. Organisation of the Paper

The rest of the structure of the paper is as follows: Section 1 contains the details of the literature review and relevant works that had taken place. Section 2 presents an overview of the associated technologies selected in the creation of the proposed system. Section 3 discusses the architecture and methodologies that were utilized. Section 4 represents the workflow in detail. Section 5 includes an overview of the objectives, use cases, and areas for improvement the system assists with. Section 6 provides future scope and suggestions for improvements and expansions. Section 7 concludes the paper with remarks, and Section 8 provides a personal reflection of the project experience.

2. LITERATURE REVIEW

Traditional recovery methods, such as posters and public announcements, have been used in the past but are inefficient, have time delays and rely on human kindness. IMEI-tracking is effective from a technical perspective, but requires coordination from telecom providers and law enforcement, and is therefore inaccessible to most users.

Research studies note the value in digitized lost and found systems that a university or airport may have utilized web-based format (often a lost + found website), which increase return rates and may do so more rapidly, but are often site-specific and not scalable to other locations/regions.

Cloud-based solutions are promising because they can store, process, and retrieve gadget information globally.Blockchain has been proposed to safely store ownership records that are verified and tamperproof, which can reduce disputes over rightful ownership.

Overall, the literature finds that individual solutions exist but there is no ecosystem that combines cloud, AI, and mobile applications that can also verify ownership securely with minimal time delay, which this project aims to propose.

3. RELATED WORK

Commercial services, such as Google’s ”Find My Device” and Apple’s ”iCloud,” have offered devicetracking services for its users. However, both are linked to their unique ecosystems, and in either case, the device must be online.

Scholars have come up with social community-based systems, the community aspect of which involved loss and found items registered by users on a voluntary basis. Such an approach is collaborative to an extent, yet, it is a service that is not very well authenticated, which presents further chances of misreporting or fraud.

4. TECHNOLOGY USED

The Smart Lost Gadget Recovery System is constructed of a blend of the latest computing technologies that combined to make the device scalable, efficient, and secure. All the technology elements have a specific role in making sure that the system does not only work but also overcomes the shortcomings of the current means of recovering gadgets.

A. Cloud Computing

The cloud computing platform is the center of the system that delivers a centralized and configurable storage of devices data. The cloud servers store important data (e.g. IMEI numbers, MAC IDs, serial number, pictures) in an encrypted manner. This provides users the ability to access their information from anywhere at any time and without using local storage. Furthermore, the cloud also allows for seamless scaling for the system to serve millions of user types at the same time.

B. Mobile Application

The application is the main user interface for both owners of gadgets and finders of gadgets. The application has been designed with accessibility and simplicity in mind to register the gadget, report lost or found, and receive notification instantly.

C. Database Security

Since sensitive information could potentially contain personally identifiable information, unique identifiers, and ownership information, supporting a strong database security is imperative. First, All user data is encrypted at rest and in transit to ensure that it's protected from unauthorized access or transmission interception. Second, part of database security is role-based account access control which ensures that only verified administrators can view and verify sensitive reports. Third, users can protect any data stored through hash and salting techniques with passwords and authentication codes.

D. Matching Engine

The matching engine is at the centre stage of the system and charged to evaluate the lost and found reports. This is accomplished through a combination technique which will encompass string-matching algorithm in cases of the ID elements such as IMEI and serial number and the computer vision algorithm to compare similarity in terms of images. An example would be when a finder sends an image of a lost smartphone, the engine will evaluate the physical characteristics of the smartphone and subsequently the data will be compared with the images that belong to the registered database.

E. Notification Services

In order to guarantee smooth and timely communication within a recovery system, we will use a multi-channel notification service. The recovery system will primarily communicate through push notifications using the mobile application, SMS messages and email messages to notify the user when a potential match has been found. The cloud messaging services will also be linked to these notification services to ensure further success in the delivery.

F. Authentication and User Verification

The platform presents more authentication methods to ensure the security of the platform and reduce the chances of misuse. Upon registration and/or logging in, an OTP verification method will be used by the user; user accounts will also be secured with the help of passwords. The temporary option of enabling two-factor authentication (2FA) is given to the users and it is supposed to offer the extra security. Administrators can play a significant role in finding possible suspicious or duplicated submissions to contribute to diminishing the risk of fraudulent claims as far as the program is concerned. Finally, all these additional authentication functions are a secure and reliable experience to everyone.

G. Scalability and Integration Potential.

The system was developed in a manner not only core technologies oriented, but also in a manner that it would be scalable and extensible. The cloud-native implementation of the system will enable the addition and removal of resources with the demand, so the purpose of the latter can be achieved with peak performance of delivery loads.

5. PROPOSED SYSTEM

The suggested system offers a universal and cloud-based, and safe lost device recovery system. Although existing solutions offer a given ecosystem, the architecture is based on interoperability, scalability and reliability. The section will describe the system architecture, functional modules, algorithms and workflow of the system.

A. System Design Philosophy the basic principle of the given system is to establish a SECURE, SCALABLE and ECOSYSTEM-AGNOSTIC digital platform through which it is possible to seamlessly integrate the registration of devices, lost-and-found reporting, and verifying owners. This solution is designed to be UNIVERSALLY COMPATIBLE unlike solutions that are only connected with one OEM or mobile operating system, which allows greater potentially uptake and viability in practice.

B. Architecture Overview

The architecture will be separated into four layers.(Fig. 1):

- Presentation Layer: End user interfaces (mobile application, web application, administration portal).
- Application Layer: Processes logic like report submission, identifier matching and image similarity computation.
- Data Management Layer: Identifier, reports, and metadata data on a cloud database which is encrypted.
- Security and Verification Layer: Makes sure that owners are validated, administrators are authorized, and that fraud is identified.

C. Module Description

The key modules of the system include:

1) User Registration and Device Enrollment: The users can create secure user profiles by using either OTP or email validation. The devices are associated with several distinctive identifiers (IMEI, MAC address, serial number) and high-resolution images. This action generates computer evidence of proprietorship.

2) Lost Gadget Reporting Module: A lost device owner will report details about the lost item including the time, the location of the last use and the distinguishing features. This is immediately uploaded in the cloud as an active search.

3) Found Gadget Reporting Module: Finders report was a module that found gadgets by photo upload and any other identifiers they may have. These reports are marked as possible matches until confirmed.

Matching and Verification Engine: The system is based on a hybrid approach:

1) Identifier Matching: IMEI/MAC/Serial numbers are checked with the help of exact and fuzzy string matching.

2) Image-Based Matching: Computer vision studies calculate similarity rates between registered and detected gadgets images.

3) Confidence Scoring: Weighted scoring is a combination of identifier and image outcomes. When the score exceeds a limit, a possible match is marked.

4) Administrator Checking: Flagged matches are checked by an administrator to avoid false positives and fraudulent claims. Confirmed cases start safe interaction between owner and finder.

5) Notification and Handover: After being verified, the owner and the finder are granted encrypted channels of communication (masked contact or secure chat). The system enables the safe recovery of the device without interference with the privacy of the user..

D. Operational Workflow

The procedure is in the following sequence:

1) Equipment is enrolled with identifiers and pictures.

2) The loss is recorded and captured in the central database.

3) Another user uploads found gadgets information.

4) The similarity score is calculated by the matching engine.

5) Admin verification is activated in case score is higher than the threshold.

6) The cases that are verified cause notification to both parties.

This workflow has real-time synchronization of the cloud modules and hence the recovery is efficient.

E. Use Case Scenario

Think of a situation when a student will lose a laptop in a university library. The student reports the device with its serial number and photo to the student immediately. One of the users subsequently comes across a laptop of similar features and uploads the report.

F. Security Considerations

The system uses:

• AES-256 identifier storage encryption.

• Role based access control (user vs.admin).

G. Comparison to Existing Systems.

The current offerings like Google and Apple are limited to brand ecosystems. Lost-and-found systems in the manual form are highly dependent on human processes and are not scalable. On the contrary, the given system is universal, automated, and has safe verification mechanisms.

H. Advantages

The proposed framework:

• Eliminates recovery time through automated matching.

• Enhances cross brand compatibility.

• Is secure with encrypted data usage. • Promotes the involvement of communities through reporting.

Finally, the offered system can be defined as a scalable and safe solution to the digital gadget recovery. Its multi-layered structure, modular structure and hybrid matching algorithms solve fundamental weaknesses of the current systems and offer a universally applicable solution..

6. METHODOLOGY

The approach taken in this project provides a balance between automation and human verification by providing effectiveness and reliability. It is made up of several interdependent modules that make up the gadget recovery workflow. The high level process is represented in figure 2.

A. System Workflow

The flow of system processes is sequential but interrelated: (1) registering a device, (2) reporting lost gadgets, (3) reporting found gadgets, (4) matching engine processes, (5) notification services, and (6) administrator verification. All the steps are closely combined with the cloud backend to provide the ability to be scaled, reliable and secure..

B. Device Registration

The journey begins with the registration of the device where the users will create a secure account within the mobile application. During the registration, users need to provide all of the required information such as IMEI number, MAC ID, serial number, brand/model of the device, and pictures of the device.

- All sensitive identifiers (IMEI, MAC ID, Serial Number) will all be stored in protected and encrypted differentia forms via AES-256 encryption.
- Multi-Factor (password plus OTP) authentication is used so that legit owners have the ability to register devices to themselves.
- All registered devices will have a record in the database with the identifier of that user and time stamp for a verifiable proof of ownership record..

This stage creates a digital footprint of the gadget which will later be used for verification and comparison.

C. Lost Gadget Reporting

When the device is reported lost the owner can provide

- Device identifiers (IMEI, MAC ID, serial number),
- Last known location (GPS coordinates if available),
- Time and date of loss, his information is stored in the cloud database. The information is recorded with an immutable timestamp. The entry is considered active in the search index and is immediately matchable.

D. Found Gadget Reporting

When a finder identifies a device that has not been claimed, they can enter the details in the mobile app or web portal. At this point:

- The finder provides text details including model, serial number (if available), and observable features.
- The finder uploads images of the device for visual verification.
- The application logs location and time created automatically.

The found device information is sent to the cloud storage and placed in queue to be compared with the lost device database..

E. Matching Engine

The matching engine is the key intelligence of the system which assists in two levels of comparison:

1) Identifier Matching: The IMEI, MAC ID and serial numbers are compared with each other via both exact and approximate string matching algorithms (e.g. Levenshtein distance to allow a degree of error tolerance). This will ensure that minor typographical mistakes do not serve as a filter to a possible match.

2) Image-Based Matching: The images uploaded are compared through the use of computer vision methods.

When either the identifier matching or image similarity surpasses a predetermined level of predetermined confidence, the system puts it on the list of potential matches.

F. Notification and Alert System

When matching is successful, the system will create an instant notification.

- When a match has been made, the system gives instant notifications. The notification of the owner is done through push notification, SMS and email.
- Any finder is also provided with confirmation that the device has been connected to a prospective owner.
- The databse entry is locked to allow further verification by an administrator.
- The multi-channel notification system implies that the users will be informed in case none of the channels of communication is effective.

G. Administrator Checking.

Necessary component to eliminate misuse and false claims is administrator verification. Upon receiving a match:

• The administrator will crosscheck the information and photographs received.

• Duplicate or fraudulent entries are processed out and filtered.

• There is a human element of intervention in this layer, which enhances trust and mitigates the possibility of controversy..

H. Case Scenario Illustration

Visualize a lost smartphone at an airport:

1) The owner promptly registers the phone via the mobile app, adding its IMEI and submitting an image of the device.
2) A finder logs details of a similar device on the same day, including a photo.
3) The matching engine establishes a perfect 100% match on IMEI, with an image match score of 92%.

The above example demonstrates how easy it is to recover belongings using the system.

I. Backend–Frontend Integration

The mobile app interfaces with the cloud server using RESTful APIs (RESTful Web Services), the back end would be implemented in Python/Node.js, the database would utilize MySql to hold structured data and MongoDB for storing unstructured data (the image).

- The recommended approach would be to store the data on AWS / Azure / GCP while gaining benefit from their datacentre scale and availability as an added benefit
- Security modules will ensure that we have endto-end encryption security of data in transit (TLS / SSL).

This modular approach ensures that the existing system is scalable, secure and user-friendly while solving the proposed problem of recovering gadgets lost in real life scenarios.

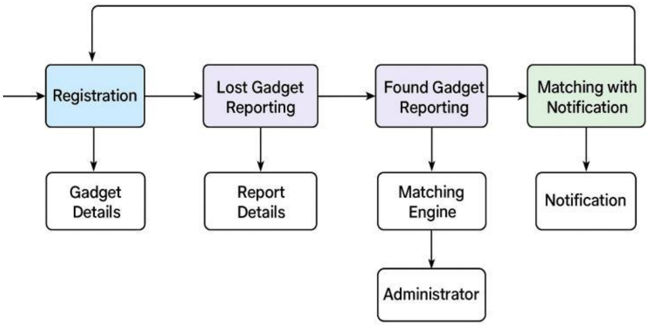

Fig. 2. Flowchart of the Gadget Recovery Process

TABLE I
COMPARISON OF EXISTING RECOVERY METHODS

Method	Cost	Reliability	Limitations
Manual Posters	Low	Very Low	Timeconsuming, local only
IMEI Tracking	Medium	High	Requires govt./telecom
Find My Device/iCloud	Free	Medium	Brand-specific, needs internet
Proposed System	Low	High	Needs internet, admin check

7. OBJECTIVES OF THE INVENTION

The key objective of a new system is to enable a global and reliable vehicle retrieval service for lost electronic devices. The system hopes to:

- Reduce the amount of time it takes for a consumer to recover a lost device.
- Increase the legitimacy of each lost device through identifiers and a photo verification process.
- Simplify and formalize the reporting protocol. • Create a secure and verified communication method between finders and owners.
- Create a scalable platform allowing for advanced and complex technologies such as AI, blockchain, and GPS.

8. APPLICATIONS

The system is usable in some real-life situations. It adds more sophistication to individuals to retrieve their own personal devices, including smartphones, laptops or tablet. Educational institutions can implement the system to improve campus and lost-and-found services within an efficient environment that will result in a minimal number of unclaimed devices on campus per year.

Employees in the corporate office access companyissued laptops and mobile phones which give the employers a mechanism of protecting the assets of their organization. The system can be built into the customer service experience of public infrastructure, including airports, bus stations, and train stations, to allow the traveler to recover lost electronic equipment. The law enforcement agencies may also find it useful as an addition to the official complaint portals, where the stolen devices can be recovered and retracted at will.

9. CHALLENGES

Despite the existence of numerous advantages with the system, the system does have shortcomings. The greatest weakness is that to use the system, one needs internet connectivity both via the mobile application and through the cloud storage. Therefore, in case the gadget is off, or is lost forever, then the system cannot retrieve it. The fraudulent reporting is another weakness. This is to say that malicious users can report a gadget as found and claim ownership yet the gadget has not been reported by finder; hence with limited items being reported, it is possible that few gadgets can be recovered.

10. FUTURE SCOPE

The Smart Lost Gadget Recovery System constitutes a powerful basis upon which the issue of lost or stolen electronic gadgets can be resolved but its prospective goes far further than the present application at present. The advanced functionality, better scalability, and extension of the platform to an increased audience can be introduced in the future as part of the research and development.

The present one authenticates gadgets by using an image-based match, however, someday, deep learning models can be created that determine gadgets based on partial, low-quality, and damaged images. AI might also be applied to detect minor features such as scratches or stickers to increase the security of a systems. Predictive models could as well be used to analyze the trends in the past as to predict the probability of recovery based on the location, device or the time of the loss, which would assist users and administrators in decision making.

One more significant opportunity involved is the use ofGPS and IoT-enabled tracking.Currently, users provide information related to their lost item when they report it, but IoT sensors or existing GPS modules could be utilized to allow real-time location tracking of the user’s possessions. Obviously there would be some restrictions as to when and how we would be able to track personal belongings, but the success rate would benefit all parties involved.

This system could also be extended not just to possessions, but also to a larger pool of lost property items that could be considered valuable assets. A couple of examples might include identity cards, keys, wallets, or travel documents. These are incredibly common items reported lost, and could all be managed on this same tracking platform. In a school or office setting, an established protocol for reporting lost cards would also improve the lost and found department's management of lost property with reduced levels of administrative work while improving time management.

Regarding scalability, the service may be expanded not only to a service for individuals but also to a national and even international network. At the community level, it can be used by universities and organizations to monitor unclaimed devices in the campuses.

Lastly, in the world, it may give the users a chance to recover a misplaced device as they travel in other countries to create a universal prototype of identifying and recovering lost devices.

The possibility of commercialization and industry alliances is also high. Insurance companies can use a trusted device register to make a smooth claim of lost or stolen devices as an example. Manufacturers of gadgets can incorporate the recovery forwarding into their products as a default option and ensure that customers become even more happy and hence loyal.

To conclude, the future of Smart Lost Gadget Recovery System is grand and extensive. The introduction of the AI, blockchain, IoT and real-time tracking produces the effect and forms a highly intelligent and reliable framework. And to add on, the diversification of other valuables, the ability to scale to national and international strategies and the cooperation with business and governments will only hasten the adoption.

11. CONCLUSION

The Smart Lost Gadget Recovery System offers a state of the art solution to an issue that is here to live. Instead of having to rely on each user individually having to trace a lost item and call the person whose item has been lost, the application brings together cloud computing, mobile applications, unique identifiers and secure authentication in a quicker and more dependable option. Provided that the app will keep adapting and evolving, it will be able to move towards an all-encompassing recovery platform enhanced by the innovative technology in a number of spheres.

12. REFLECTIONS

Being part of this project taught the team a lot of valuable lessons associated with problem solving in the real world. It has pushed the entirety of our knowledge in the field of cloud computing, cyber security and development of mobile apps. A more challenging experience has been associated with creating the database in a manner that allowed the storage of sensitive data to include IMEI and MAC IDs without suffering significant losses by having to use slow access to compare the outcomes. In general, it was an excellent learning experience and it developed our technical and problem solving abilities.

References

1. R. Buyya, C. Vecchiola, and S. Thamarai Selvi, "Mastering Cloud Computing," McGraw Hill, 2013.
2. R. Buyya, J. Broberg, and A. Goscinski, "Cloud Computing: Principles and Paradigms," Wiley, 2011.
3. S. Russell and P. Norvig, "Artificial Intelligence: A Modern Approach," 3rd ed., Pearson, 2010.
4. A. Bahga and V. Madisetti, "Internet of Things: A Hands-On Approach," Universities Press, 2015.
5. M. Swan, "Blockchain: Blueprint for a New Economy," O'Reilly Media, 2015.

6. W. Stallings, "Cryptography and Network Security," 7th ed., Pearson, 2016.
7. R. S. Pressman, "Software Engineering: A Practitioner's Approach," 7th ed., McGraw-Hill, 2010.
8. A. Kumar and R. Sharma, "Cloud-Based Lost and Found Item Tracking System," *International Journal of Computer Applications*, vol. 182, no. 3, pp. 15-20, 2018.
9. S. Gupta et al., "A Smart Framework for Lost Mobile Tracking," *IEEE International Conference on Computational Intelligence*, pp. 112–117, 2019.
10. J. Redmon and A. Farhadi, "YOLOv3: An Incremental Improvement," arXiv:1804.02767, 2018.
11. K. Simonyan and A. Zisserman, "Very Deep Convolutional Networks for Large-Scale Image Recognition," arXiv:1409.1556, 2014.
12. H. Garcia-Molina, J. Ullman, and J. Widom, "Database Systems: The Complete Book," 2nd ed., Pearson, 2008.
13. B. Hofmann-Wellenhof, H. Lichtenegger, and E. Wasle, "GNSS – Global Navigation Satellite Systems: GPS, GLONASS, Galileo, and More," Springer, 2007.
14. K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
15. Z. Xiao and Y. Xiao, "Security and Privacy in Cloud Computing," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 2, pp. 843–859, 2013.
16. P. G. Ipeirotis, "Demographics of Mechanical Turk," NYU Stern School of Business, Working Paper, 2010.
17. I. Goodfellow, Y. Bengio, and A. Courville, "Deep Learning," MIT Press, 2016.
18. W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge Computing: Vision and Challenges," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637–646, 2016.
19. H. Chourabi et al., "Understanding Smart Cities: An Integrative Framework," *IEEE 45th Hawaii International Conference on System Sciences*, pp. 2289–2297, 2012.
20. R. Kshetri, "The Emerging Role of Big Data in Key Development Issues: Opportunities, Challenges, and Concerns," *Big Data & Society*, vol. 1, no. 2, pp. 1–20, 2014.
21. G. Navarro, "A Guided Tour to Approximate String Matching," *ACM Computing Surveys*, vol. 33, no. 1, pp. 31–88, 2001.
22. W. Zhao, R. Chellappa, P. J. Phillips, and A. Rosenfeld, "Face Recognition: A Literature Survey," *ACM Computing Surveys*, vol. 35, no. 4, pp. 399–458, 2003.
23. C. Bishop, "Pattern Recognition and Machine Learning," Springer, 2006.
24. A. Tanenbaum and D. Wetherall, "Computer Networks," 5th ed., Pearson, 2011.
25. Anbumani. P, Vasantharaja. R, Gokul. MP, Roopesh. VS, Hareesh SD. Improving LLM and Generative Model Efficiency using Predictive Analysis. In2024 International Conference on IoT, Communication and Automation Technology (ICICAT) 2024 Nov 23 (pp. 69-73). IEEE.
26. S. Prabakaran, V. Shangamithra, G. Sowmiya, R. Suruthi, Advanced smart inventory management system using IoT, International Journal of Creative Research Thoughts (IJCRT), vol 11, Issue 4, page 37-45