Industrial Asset Management using RFID

Aditya Agrawal
Dept. of Computer Science & Engineering
Dr. Akhilesh Das Gupta Institute of Technology and Management, Delhi, India

Jai Garg
Dept. of Electronics & Communication Engineering
Dr. Akhilesh Das Gupta Institute of Technology and Management, Delhi, India

Prof. (Dr.) Anupam Sharma
Dept. of Computer Science & Engineering
Dr. Akhilesh Das Gupta Institute of Technology and Management, Delhi, India

Prof. (Dr.) Rajiv Sharma
Dept. of Electronics & Communication Engineering
Dr. Akhilesh Das Gupta Institute of Technology and Management, Delhi, India

***Abstract*:- The paper outlines implementation of a secure industrial asset management system using Ultra High Frequency Radio Frequency Identification. The system methodology places emphasis on security and usability of the system. To conveniently facilitate updation and movement of assets without using an RFID reader, the paper describes the use of QR code.**

Keywords:- Asset Tracking, RFID, Web Security, Web Usability

INTRODUCTION

Traditionally asset management has been done using Barcode [1] and associated methods. Asset security in most industries is implemented using physical security checkpoints aided by security personnel. Prior implementation of asset tracking has been done using RFID systems[2] and WLAN[3]. These systems have lacked essential management features like a user interface and security alerts.

Use of modern web technologies in conjunction with low power modern microcontrollers can provide an effective mechanism for asset management. Implementation of three tier web architecture enables the system to be scalable and fault tolerant. Use of modern responsive web technologies to create the user interface ensures greater adaptability, acceptability and consistency. The aforementioned model also eliminates duplication of effort in conventional systems that posed the need for a separate website optimized for handheld devices.

With close to 700 million internet users in India [4] and a similar number of smartphones in the country, it makes sense to implement a mobile first approach in the system. The availability of a camera in addition to GPRS support in almost all modern smartphones allows us to use QR code in conjunction with UHD RFID in the system for enhanced convenience.

Finally, considering the sensitive nature of asset tracking systems, it is trivial to develop a secure system that is resilient against common web attacks.

HARDWARE ARCHITECTURE

The RFID tags deployed in the project use the 915MHz frequency band with the maximum operating distance of 10 metres from the reader. Ultra High Frequency is used because it supports high speed data transfer upto 128kbps. Prior research shows that UHF RFID can perform remarkably well at operating distance of upto 6 feet in terms of error rate[5]. Whenever a device or an asset is to be registered to the database, a tag is attached to the asset and is scanned to be added to the DB. This helps in detecting movement of the asset in a premises where multiple UHF RFID readers are installed to track and manage movement of each asset.

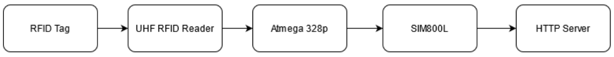


Fig. 1 Hardware Architecture Flowchart

Fig.1 shows the complete flow of our main system. To eliminate the need of an RFID reader everytime the asset information needs to be updated, we implement the use of a QR Code. QR codes also facilitate easy high speed detection using handheld smartphones without worrying about alignment of the reader [6]. Each asset has a tamper proof QR code sticker installed on it which is linked to the asset and RFID tag at the time of registration. To update any information about the asset user can scan the QR code via the desktop or mobile application and can then perform requisite operations like updating or accessing the asset information based on the role based access control policy.

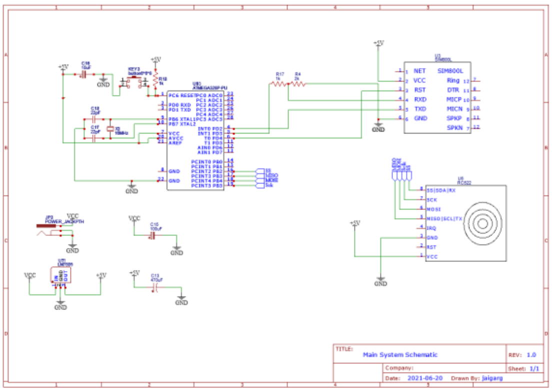


Fig. 2 Main System PCB Schematic

In developing economies like India, GSM has better network coverage compared to LTE which is still catching up[7]. This is the reason the SIM800L module[8] has been used for communication with the API Server. SIM800L module works on frequencies GSM850MHz, EGSM900MHz,PCS1900MHz and DCS1800MHz. It is a quad band GSM/GPRS Module. The communication system uses this module to send and receive asset data from the API server. When an asset is detected by the UHF RFID Receiver, an SPI interrupt calls an ISR on the main system which in turn

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

sends a trigger to the API server in form of an HTTPS request to keep track of the moving asset.

Fig.2 Shows the PCB Schematic of the main system. The system uses AtMega328p, a low power 8 bit microcontroller based on AVR RISC architecture[9]. The microcontroller communicates with the UHF RFID reader over SPI Communication channel. The microcontroller communicates with the SIM800L module using software defined serial port. This configuration is optimal because native support for SPI leads to a lower error rate for RFID[10]. Moreover, the GSM module is a secondary device which is used only when the data is being sent to the API server. The UART port of the microcontroller is left unconnected for debugging and testing purposes.

SOFTWARE ARCHITECTURE

The software implements a three tier architecture to support flexibility and scalability[11]. The backend of the software has been created using Django. Django is a web development framework based on Python that allows for quick development of secure web applications[12.] For the data storage, we use PostgreSQL because of its support for custom data types [13] including lists that allow for fast traversal of updation history of assets. The front end is based on Responsive web design principles using Bootstrap. Bootstrap allows the use of a flexible grid system to display the content uniformly to users across various devices[14]. We use serializers to properly format output in JSON and to validate and transform input JSON to native python data types.Additionally, in line with REST API best practices [15], the use of Django routers and viewsets facilitate clean URIs that communicate the API resource model to developers while allowing for CRUD operations on the same URI using appropriate HTTP methods. The system allows the following operations

1. Login
2. Creating Assets
3. Retrieving Assets
4. Updating Assets
5. Deleting Assets
6. Listing Assets
7. Viewing Summary

Apart from login, as outlined in Fig. 3, all the operations need the request to be authenticated using the Authorization cookie and the user needs to have access to perform the said operation.

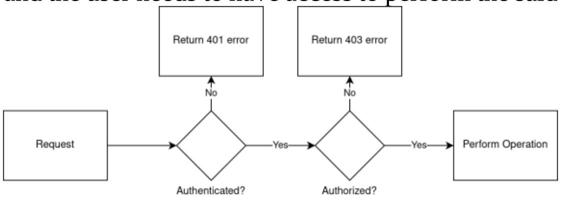
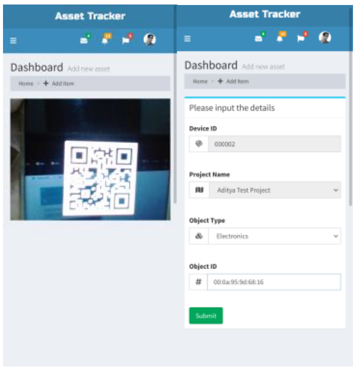


Fig. 3 Software Architecture Flowchart

The system is deployed using gunicorn which is a WSGI server for UNIX based systems. Gunicorn allows for multiple synchronous workers with multithreading support.



Please input the details

Device ID: 000002

Project Name: Aditya Test Project

Object Type: Electronics

Object ID: 00:0a:95:9d:68:16

USABILITY CONSIDERATIONS

The data has been displayed on the website using ChartJS in line with visualization best practices. Multiple temporal series of cost and expenditure analysis have been plotted on differently shaded line charts [16].

Responsive Web Design (RWD) methodology has been implemented in the project with emphasis on the mobile first approach. RWD allows for a consistent experience across various devices. To facilitate better user retention[17], the web page makes use of lazy loading of images and deferred loading of javascript files. In addition, static assets are cached to allow for faster subsequent access. Moreover, the application uses django thumbor to dynamically resize images according to the user device.

SECURITY CONSIDERATIONS

To mitigate insecure direct object reference (IDOR) vulnerability[18], we encrypt the QR code using AES 256 encryption.

Considering the inherent sensitivity associated with asset management systems, two factor authentication using SMS is implemented in the system [19] which allows for mitigation of keylogging attacks in the system [20] and improves the confidence of the user in the system.

Role based access control is implemented to enforce authorization [21] In our system, this is implemented by creating groups and assigning users to one of these groups. These groups act as roles with a defined level of access to the various API endpoints. Session management poses inherent risks in token generation and session management mechanisms [22]. To combat vulnerabilities pertaining to Token generation, Mersenne Twister[23] along with OS Specific randomness generation available in the Python library is used as the Pseudo Random Number Generator (PRNG) to generate the token for the user. Implementation of the system on UNIX based systems make use of the urandom pool which uses device driver noise for entropy as the seed to Mersenne Twister. To mitigate the flaws in the session management mechanisms, the use of HttpOnly attribute is used to limit the scope of authentication cookies to HTTP requests[24]. Moreover, the use of HTTP Strict Transport Security (HSTS) is enforced to force clients to connect to the server over HTTPS connection to prevent click through vulnerability. [25]

CONCLUSION

Ultra High Frequency RFID based systems can be effectively used in domains like industries, institutions and hospitals to

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

effectively manage physical assets. The use of Quick Response(QR) codes can eliminate the need of having an RFID reader for updating the assets and can provide a manifold increase in productivity. The three tier web architecture ensures that the system can easily scale horizontally and handle thousands of requests per second from the array of sensors. These systems can effectively provide high usability to new users following techniques outlined in the ISO 9241-11:2018 standard by implementing techniques that improve the effectiveness, efficiency and satisfaction of the system. Responsive Web Design (RWD) can effectively provide users with a consistent experience and increase retention time. Furthermore, implementation of security best practices can provide resilience against attacks mentioned in the OWASP Top 10 repository[26].

FUTURE SCOPE

The use of ceramic tamper proof RFID tags may be explored in the system to provide a higher level of physical security. In addition, deployment of the application to robust infrastructure with failover using modern web technologies may be implemented. Finally, the development of the application may be done natively for android and iOS platforms for the performance and usability improvement it provides[27].

REFERENCES

[1] S. Lin and P. Wang, "Design of a barcode identification system," 2014 IEEE International Conference on Consumer Electronics - Taiwan, 2014, pp. 237-238, doi: 10.1109/ICCE-TW.2014.6904077.

[2] Evizal, Evizal, and Sharul Kamal Abdul Rahim. "Active RFID Technology for Asset Tracking and Management System." *TELKOMNIKA. Yogyakarta* 11 (2013): 137-146.

[3] J. Youn, H. Ali, H. Sharif, J. Deogun, J. Uher and S. H. Hinrichs, "WLAN-Based Real-Time Asset Tracking System in Healthcare Environments," Third IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2007), 2007, pp. 71-71, doi: 10.1109/WIMOB.2007.4390865.

[4] Agrawal, Ravi. *India connected: how the smartphone is transforming the World's largest democracy*. Oxford University Press, 2018.

[5] Buettner, Michael, and David Wetherall. "An empirical study of UHF RFID performance." *Proceedings of the 14th ACM international conference on Mobile computing and networking*. 2008.

[6] Soon, Tan Jin. "QR code." *Synthesis Journal* 2008 (2008): 59-78.

[7] Poranki, K.R., Perwej, Y. and Perwej, A., 2015. The level of customer satisfaction related to GSM in India. *Research Journal of Science & IT Management*, *4*(3), pp.30-36.

[8] https://simcom.ee/documents/SIM800/SIM800_Hardware%20Design_V1.09.pdf

[9] Turley, Jim. "Atmel avr brings risc to 8-bit world." *Microprocessor Report* 11.9 (1997): 4.

[10] DAyAl uDAi, Arun. "SeriAl CommuniCAtionS with AVr miCroController."

[11] John M. Gallaugher & Suresh C. Ramanathan (1996) Choosing a Client/Server Architecture, Information Systems Management, 13:2, 7-13, DOI: 10.1080/10580539608906981

[12] Holovaty, Adrian, and Jacob Kaplan-Moss. *The definitive guide to Django: Web development done right*. Apress, 2009

[13] Conrad, Tim. "Postgresql vs. mysql vs. commercial databases: It's all about what you need." (2006).

[14] Spurlock, Jake. *Bootstrap: responsive web development*. " O'Reilly Media, Inc.", 2013.

[15] Masse, Mark. *REST API Design Rulebook: Designing Consistent RESTful Web Service Interfaces*. " O'Reilly Media, Inc.", 2011.

[16] Luo, X., Yuan, Y., Zhang, K. *et al*. Enhancing statistical charts: toward better data visualization and analysis. *J Vis* 22**,** 819–832 (2019).

[17] Gardner, Brett S. "Responsive web design: Enriching the user experience." *Sigma Journal: Inside the Digital Ecosystem* 11.1 (2011): 13-19.

[18] Gupta, Shashank and B. B. Gupta. "Detection, Avoidance, and Attack Pattern Mechanisms in Modern Web Application Vulnerabilities: Present and Future Challenges." *IJCAC* vol.7, no.3 2017: pp.1-43. http://doi.org/10.4018/IJCAC.2017070101

[19] F. Aloul, S. Zahidi and W. El-Hajj, "Two factor authentication using mobile phones," 2009 IEEE/ACS International Conference on Computer Systems and Applications, 2009, pp. 641-644, doi: 10.1109/AICCSA.2009.5069395.

[20] D. Nyang, A. Mohaisen and J. Kang, "Keylogging-Resistant Visual Authentication Protocols," in IEEE Transactions on Mobile Computing, vol. 13, no. 11, pp. 2566-2579, Nov. 2014, doi: 10.1109/TMC.2014.2307331.

[21] Gail-Joon Ahn and Ravi Sandhu. 2000. Role-based authorization constraints specification. *ACM Trans. Inf. Syst. Secur.* 3, 4 (Nov. 2000), 207–226. DOI:https://doi.org/10.1145/382912.382913

[22] Vollbrecht, John, et al. *AAA authorization framework*. rfc 2904, August, 2000.

[23] C. A. Vlsaggio and L. C. Blasio, "Session management vulnerabilities in today's web," in IEEE Security & Privacy, vol. 8, no. 5, pp. 48-56, Sept.-Oct. 2010, doi: 10.1109/MSP.2010.114.

[24] Makoto Matsumoto and Takuji Nishimura. 1998. Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator. *ACM Trans. Model. Comput. Simul.* 8, 1 (Jan. 1998), 3–30. DOI:https://doi.org/10.1145/272991.272995

[25] Barth, Adam. "HTTP state management mechanism." (2011).

[26] Hodges, Jeff, Collin Jackson, and Adam Barth. "Http strict transport security (hsts)." *URL: http://tools. ietf. org/html/draft-ietf-websec-strict-transport-sec-04* (2012).

[27] OWASP Top Ten https://owasp.org/www-project-top-ten/

[28] Charland, Andre, and Brian Leroux. "Mobile application development: web vs. native." *Communications of the ACM* 54.5 (2011): 49-53.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)