

Digitalization in India Using RFID Technology with Internet of thing

^{#1}Prof. Takale D.G., ^{#2}Miss.Yogita Pardeshi, ^{#3}Miss.Hole Dipali,
^{#4}Mr.Shelar Nilesh.



¹yogitapardeshi1223@gmail.com

²holedipali14@gmail.com

³shelarnilesh109@gmail.com

^{#1234}Department of Computer Engineering,

Dattakala Group of institutions Faculty of Engineering, Swami Chincholi

ABSTRACT

Now a day's people are dependent on digital way of doing any work. But there is still one case where we are using papers for doing that work which is related to educational, medical etc. Peoples carry le of documents while going for work such as for issuing driving license. There is one solution on this problem by replacing bunch of documents with just single RFID card. A data security integrated system, based on the server, which uses RFID technology to combine functions of physical access control, computers access control and management. Using RFID Reader for scanning particular person there are also chances of fraud. This can overcome using Fingerprint sensor. Suppose that the security level of such digital signature system can be further increased using RFID tags in addition to smart digital services. This allows preventing an unauthorized use of the smart card carrying the secret key. Intellectual RFID tags can help us when a physical access control system is not installed or when it is impossible or inexpedient to connect such system to the digital signature system and the computers access control and management system. This tag is an additional authentication factor required to gain permission to use the cryptographic smart card for signing a document. The presence detection/access control function is comprised of a wired/wireless sensor network of readers that is installed to detect person information with tags.

Keyword: Digital signature, Access control, RFID, Smart cards

ARTICLE INFO

Article History

Received: 22nd April 2019

Received in revised form :
22nd April 2019

Accepted: 25th April 2019

Published online :

29th April 2019

I. INTRODUCTION

In daily life the processes or services which are especially for the people, to get these services properly and within time is important. If people go to buy a SIM card to mobile shop, then they have to cross verify the fingerprint of that particular user or customer with the Adhar card number. There are so many such services which take too much time, manpower and system resource. Such services are related to RTO, College admission, Bank, Passport and so many. These all services are only for the peoples but these are so time consuming and there are also the chances of fraud in getting services. So it is important to make all services digital. Proposed system uses server as cloud for storing the necessary documents. The particular documents they use where they become necessary. This can overcome using

Fingerprint sensor. Suppose I opening an account in bank then I need to just carry a RFID tag .

II. PROBLEM STATEMENT

For Public Sector and Government Agencies, with tens or hundreds of thousands of documents, a document management system is becoming a mandate to organize, index and control their documents in a hassle free manner. Public Sector and Government Agencies deal with Documents which range from Public View documents, Tenders, to the most Confidential and Secret Documents which are intended only for view of certain designated personnel. Storing all these documents as physical records not just consumes a lot of space but also is a tedious an air to let these documents and manage them safely with restricted access. So we are providing one digital solution to

this problem with RFID card and fingerprint scanner. User will get authenticated by unique id of RFID associated with each document.

a. Project Scope :

We can create global Database, so that different services can be accessible globally. Intellectual RFID tags with possibility of strong mutual authentication with smart cards allow to provide unauthorized access to digital signature secret keys: they can be used after successful mutual authentication only. We proposed several ways to combine RFID-based physical access control systems with digital signature systems to increase their security, including improved digital signature calculation procedure that allows to prevent unauthorized calculation of a digital signature for a fraudulent document.

b. Objectives:

To provide smarter way for our important document storage and handling. By using RFID and Fingerprint we will provide security to system. Main objective is to reduce problems regarding document handling such as document misplacement, waiting in queue for verification.

III. LITERATURE SURVEY

TTILE	AUTHOR	YE AR	REVIEW
IDStack - the Common Protocol for Document Verification Built on Digital Signatures	Chanaka Lakmal and Sachithra Dangalla	2017	The need for a better solution for document verification in the Sri Lankan context is clear and expanding. With the advancement in the use of digital documents, document verification has a very good potential to grow in many directions.
Digital Signature On File Using Biometric Fingerprint With Fingerprint Sensor On Smartphone	Erika Rahmawati and Mariska Listyarsari	2017	Fingerprint on smartphone can perform encryption and decryption process by connected to the server and call the PHP program functions.
How to Sign Multiple Versions of Digital Documents	AmrilSy alimb and Kouichi Sakurai	2017	In this paper, we have proposed a more efficient method to sign multiple versions of digital documents. We have proposed a signature scheme based on RSA and showed that the scheme is secure in the random oracle model. The advantages of our method are:

Combining RFID-Based Physical Access Control Systems with Digital Signature Systems to Increase Their Security	AndreyL archikov, Sergey Panasenko	2016	Using RFID technology in digital signature schemes allows to increase their security. Even low-end RFID tags can add one more security level when combined with physical access control systems.
--	------------------------------------	------	--

Table1 :Literature Survey

Keystroke Dynamics, The essentials of keystroke dynamics is not what you type, but how you type. In this paper, it mainly presents our proposed authentication system supporting with keystroke dynamics as a biometric for authentication. We use inter-key delays of the password and the account for user identification in the system design. Design of a secure digital recording protection system with network connected devices. We present a new recording protection system for network connected devices that belong to a user's personal network.

An Intranet-Based Document Management and Monitoring System Framework:

A Case for the National University Quality Management Office it provides a framework where the development of an Intranet based Documents Management System can be based. Combining RFID-Based Physical Access Control Systems with Digital Signature Systems to Increase Their Security. In this paper it uses RFID technology to combine functions of physical access control, computers access control and management, and digital signature systems. This combination allows to drastically increase systems security. Software defined radio based implementation of RFID tag in next generation mobile we present development and implementation of the Software Defined Radio (SDR) active backscattering tag compatible with the EPCglobal UHF Class 1 Generation 2 (Gen2) RFID standard. Decentralized Mobile SNS Architecture and Its Personal Information Management Mechanism. Mobile SNS is one of the most popular topics of mobile Internet. In order to fulfill the user demand for self-maintained independent social network and ensure the privacy of their personal information and resources, the paper proposes system architecture of decentralized mobile SNS.

IV. PROPOSED SYSTEM

The basic flow of the projects depends upon the scenarios present and items which work accordingly to build upon greater tasks. The section gets divided to derive out all the information from the work flows. When building upon such data sets a proper generation of categories must be done to solve problems. The first scenario comes of the

customer as he is using the application made by the developer and then uses its full potential for his benefit.

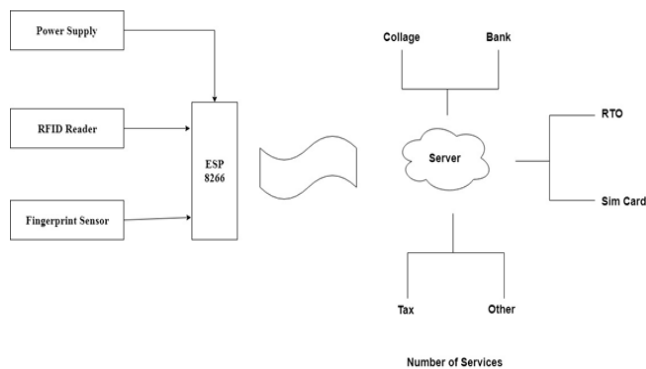


Fig1. : System Architecture

RFID :

Radio-Frequency Identification (RFID) is the use of radio waves to read and capture information stored on a tag attached to an object. A tag can be read from up to several feet away and does not need to be within direct line-of-sight of the reader to be tracked. Radio-frequency identification (RFID) uses electromagnetic fields to automatically identify and track tags attached to objects. The tags contain electronically stored information. Passive tags collect energy from a nearby RFID reader's interrogating radio waves. Active tags have a local power source (such as a battery) and may operate hundreds of meters from the RFID reader. Unlike a barcode, the tag need not be within the line of sight of the reader, so it may be embedded in the tracked object. RFID is one method of automatic identification and data capture (AIDC).

RFID Tag :

A radio-frequency identification system uses tags, or labels attached to the objects to be identified. Two-way radio transmitter-receivers called interrogators or readers send a signal to the tag and read its response. RFID tags can be either passive, active or battery-assisted passive. An active tag has an on-board battery and periodically transmits its ID signal. A battery-assisted passive (BAP) has a small battery on board and is activated when in the presence of an RFID reader. A passive tag is cheaper and smaller because it has no battery; instead, the tag uses the radio energy transmitted by the reader. However, to operate a passive tag, it must be illuminated with a power level roughly a thousand times stronger than for signal transmission. That makes a difference in interference and in exposure to radiation.

Tags may either be read-only, having a factory-assigned serial number that is used as a key into a database, or may be read/write, where object-specific data can be written into the tag by the system user. Field programmable tags may be write-once, read-multiple; "blank" tags may be written with an electronic product code by the user. RFID tags contain at

least three parts: an integrated circuit that stores and processes information and that modulates and demodulates radio-frequency (RF) signals; a means of collecting DC power from the incident reader signal; and an antenna for receiving and transmitting the signal. The tag information is stored in a non-volatile memory. The RFID tag includes either fixed or programmable logic for processing the transmission and sensor data, respectively.

RFID Reader :

RFID systems can be classified by the type of tag and reader. A Passive Reader Active Tag (PRAT) system has a passive reader which only receives radio signals from active tags (battery operated, transmit only). An Active Reader Passive Tag (ARPT) system has an active reader, which transmits interrogator signals and also receives authentication replies from passive tags.

An Active Reader Active Tag (ARAT) system uses active tags awoken with an interrogator signal from the active reader. A variation of this system could also use a Battery-Assisted Passive (BAP) tag which acts like a passive tag but has a small battery to power the tag's return reporting signal. Fixed readers are set up to create a specific interrogation zone which can be tightly controlled. This allows a highly defined reading area for when tags go in and out of the interrogation zone. Mobile readers may be hand-held or mounted on carts or vehicles.

Fingerprint:

A fingerprint in its narrow sense is an impression left by the friction ridges of a human finger. The recovery of fingerprints from a crime scene is an important method of forensic science. Fingerprints are easily deposited on suitable surfaces (such as glass or metal or polished stone) by the natural secretions of sweat from the eccrine glands that are present in epidermal ridges.

In a wider use of the term, fingerprints are the traces of an impression from the friction ridges of any part of a human or other primate hand. A print from the sole of the foot can also leave an impression of friction ridges. Deliberate impressions of fingerprints may be formed by ink or other substances transferred from the peaks of friction ridges on the skin to a relatively smooth surface such as a fingerprint card. Fingerprint records normally contain impressions from the pad on the last joint of fingers and thumbs, although fingerprint cards also typically record portions of lower joint areas of the fingers.

ESP8266 :

The ESP8266 is a low-cost Wi-Fi microchip with full TCP/IP stack and microcontroller capability produced by manufacturer Espressif Systems in Shanghai, China. The chip first came to the attention of western makers in August 2014 with the ESP-01 module, made by a third-party manufacturer Ai-Thinker. This small module allows

microcontrollers to connect to a Wi-Fi network and make simple TCP/IP connections using Hayes-style commands. However, at first there was almost no English-language documentation on the chip and the commands it accepted. The very low price and the fact that there were very few external components on the module, which suggested that it could eventually be very inexpensive in volume, attracted many hackers to explore the module, chip, and the software on it, as well as to translate the Chinese documentation. The ESP8285 is an ESP8266 with 1 MB of built-in flash, allowing for single-chip devices capable of connecting to Wi-Fi.

V. CONCLUSION

We can create global cloud using ESP8266, so that different services can be accessible globally. Intellectual RFID tags with possibility of strong mutual authentication with smart cards allow to provide unauthorized access to digital signature secret keys: they can be used after successful mutual authentication only. We proposed several ways to combine RFID-based physical access control systems with digital signature systems to increase their security. Including improved digital signature calculation procedure that allows preventing unauthorized calculation of a digital signature for a fraudulent document.

ACKNOWLEDGMENT

I want to thank all people who help me in different way. Especially I am thankful to my guides "Prof. Takale D.G." for his continuous support and guidance in my work. Also, I would like to thank DGOIFOE College Computer Department HOD "Prof. Rajpure A.S." and PG-Cordinator "Prof. Bere S.S." Lastly.

REFERENCES

1. "Combining RFID-Based Physical Access Control Systems with Digital Signature Systems to Increase Their Security". P. Solic, J. Radic, N. Rozic
2. An Intranet-Based Document Management and Monitoring System Framework: A Case for the National University Quality Management OcéAndreyLarchikov, Sergey Panasenko, Alexander V. Pimenov, PetrTimofeev(2016).
3. "Software dened radio based implementation of RFID tag in next generation mobiles" IEEE Transactions on Consumer Electronics, vol. 58, no. 3, pp. 1051-1055, August 2012.
4. Decentralized Mobile SNS Architecture and Its Personal Information Management Mechanism. 2016K. Balakarhik