**LITERATURE SURVEY**

It's generally common knowledge that, if security controls are too onerous or interfere too much with people's everyday work, employees will try and circumvent them or ignore them whenever they can. This is one reason why automatic identification, or auto ID, for short, is quickly gaining popularity: It offers convenience in security, identification and access control, particularly physical access control. Auto ID is often combined with automatic data capture to increase efficiency, reduce data entry errors and free up staff.

Auto ID covers a variety of technologies, including barcodes, magnetic stripes, smartcards, radio frequency identification (RFID) and biometric technologies, such as voice recognition. RFID technology has been widely used in stock control, but its use is spreading to ID cards for personnel as well, as it has the advantage of contactless authentication, which is great for door access where hands-free operation is preferred or needed.

With systems such as barcodes, magnetic stripes and proximity readers, individuals must hold the badge against (or close to) the scanner, as these use line-of-sight technology. The readers can only read one badge at a time, and any embedded information cannot be dynamically changed.

RFID ID badges can be read from much farther distances than other traditional technologies and don't require the tag to be oriented in a particular way. Most systems have anti-collision capabilities, so they can read several tags at the same time. Badges come in various form factors, and can be clipped-on, or attached with a wristband or neck loop.

A typical [RFID system](https://searcherp.techtarget.com/feature/Radio-frequency-identification-tags-technology-finds-supply-chain-niche) consists of an RFID microchip with an antenna -- called a tag -- a reader with an antenna, and an access control server. If the system is using passive RFID tags, which have no battery, the reader sends out electromagnetic waves, which the tags' antennae are tuned to receive. The tags draw power from the magnetic field created by the reader and use this power to activate the microchip to send data back to the reader. An active RFID tag has its own battery power and so can periodically transmit the data stored on it to the RFID reader.

The RFID reader cross-references the tag's data within its own database or sends it wirelessly to the server. The read range depends on the frequency and type of tag. Some readers can cover a total area of up to 30,000 square feet. Wireless RFID scanners allow the readers to be relocated or repositioned as needs change.

The most common method of authentication using an RFID system is to store a serial number unique to the user, but tags can also be used to store biometric information, such as a photograph. CCTV can then compare an individual's face with the image stored on the RFID to authenticate someone at an unmanned entry point, or to regulate access depending on the time of day. RFIDs can also trigger CCTV cameras to capture unauthorised or authorised access in real-time, or when certain RFID events occur, such as someone tampering with an RFID badge.

Access information can be tied to data in Windows Active Directory or LDAP for user authentication, and therefore be synchronised to an authorised access scheme. As well as controlling access to restricted areas, RFID can easily track time and attendance, as well as employee and visitor location. By having a fully integrated access system, physical and logical access can be tightly controlled and comprehensive audit logs generated. For example, RFID logs can be used to check patrols by guards to ensure individuals complete them as per their rota. Also, in an emergency, a real-time map can show the location of key personnel.

[RFID systems](https://searcherp.techtarget.com/video/Webcast-Getting-started-with-RFID-in-manufacturing) can easily be adapted to most environments that require restriction of access or movement of personnel. For employees, the big advantage is they are truly hands-free, eliminating the need to hold the badge or pass next to a scanner.

One problem with [RFID technology](https://searcherp.techtarget.com/feature/RFID-market-expanding-with-new-technology-options) relates to standards. RFID can use different frequencies, but the most common are low, high or UHF. There are standards for low- and high-frequency RFID systems, but most companies want to use UHF in the supply chain, because it offers a longer read range. However, many other types of devices use the UHF spectrum -- meaning their signals interfere with each other, so RFID readings become inaccurate or non-existent -- and an accepted standard is still some way off.

There are also some [RFID security concerns](http://searchsecurity.techtarget.co.uk/tip/RFID-security-issues-endanger-companies-and-consumers): It is possible for RFID tags to be read by unauthorised readers, accessing any personal information stored on them, for example where people are close together on a crowded train. Users can guard against this kind of 'skimming' by requiring passwords in order to access a tag’s memory or enforcing encryption between the tag and reader. In the US, the NIST standard FIPS 201 requires that RFID Personal Identity Verification cards be kept in a FIPS 201-approved, shielded badge holder, which prevents unauthorised reads.

RFID technology can deliver a convenient hands-free access control and automated data capture solution with many advantages over traditional access control badges and systems. It may sound a bit Big Brother, but it can be appropriate in critical or sensitive areas, particularly where a physical perimeter defence plays an important role. Like most technologies, RFID is developing quickly, and any [RFID projects](http://searchsecurity.techtarget.co.uk/answer/RFID-tags-Do-they-have-a-secure-future) will require advice from an experienced vendor in order to select the right type of tag for specific environments and uses. The good news, however, is that, as the technology becomes more popular, it is also becoming more affordable.

RFID stands for **Radio Frequency Identification**. RFID technology makes use of electromagnetic waves to capture and read data. The information is electronically stored on a tag that is attached to an object or the carrier. The tags can be detected from several feet away by the receiver.

RFID technology is popularly employed in access control systems to allow entry of authentic and authorized personnel only.

RFID technology has application in several areas such as:

* Identification of personnel
* Access based security systems
* Parking facilities including gate control
* Tracking of consumer goods

RFID in Access Control Management as Attendance System

The most common use of RFID is in access control as an attendance system over a website. The basic principle upon which RFID tags are employed is the identification badge of the workers of any company or industry. The RFID applications for personnel identification uses normally quite low frequency, almost 140 KHz, for badge detection.

Let’s take a deeper dive to understand how RFID technology works in the access control systems. RFID system is composed of the following [**main components**](https://www.getkisi.com/resources/components):

* The RFID Card or Tag
* The RFID Reader
* Card Access Management Software
* Access Control Panel
* Buzzer

**RFID Card / Tag**

The information of person, object or the carrier is electronically stored in the RFID cards/tags. The RFID card/tag can contain only small piece of information such as identification number, price or code.

**RFID Reader**

The RFID reader has an antenna which sends the radio waves to detect any RFID tag or card within its range. This range can vary for the RFID readers depending upon the frequency of emitted radio waves.The RFID reader decodes the uniquely stored information in the RFID card/tag and sends the signal to the host software.



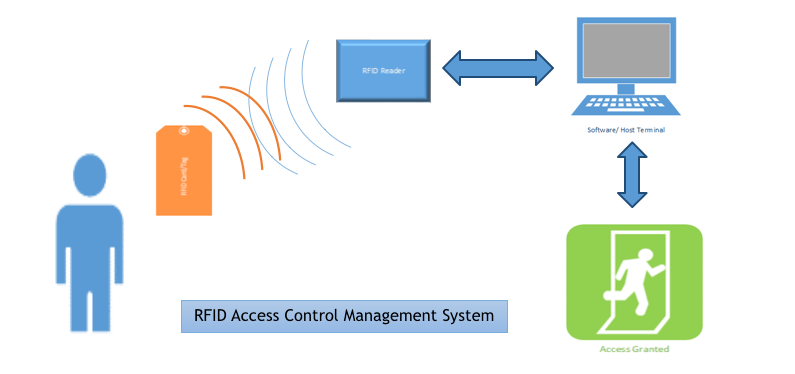
**Fig no. 1:RFID System**

**Software / Infrastructure**

The software system reads the signal received from RFID reader and grants or rejects the access of system to the person.

**Access Control Panel/Webpage**

[Access control panel](https://www.getkisi.com/guides/access-control-panels) is not a basic part of RFID system. Access control panel hardware is needed to mark or authorise the user, when the access is granted to the authorized personnel.



**Fig No.2 :RFID Access Control Management System**

‍Pros and Cons of RFID Technology

Every technology comes with a pro and a flip side. Same goes for the RFID technology.

**RFID technology offer the following benefits:**

RFID chips are small enough to be implanted underneath a person’s skin without the possibility of any sort of discomfort. This technology can be used to track fugitives, and store the medical and health data of a person and use it, if required. RFID chips are robust when compared with the bar codes. No fear of wear and tear condition as the RFID card would still be able to send the information. RFID tags can function virtually in any kind of situation or weather.

**The cons of RFID technology are discussed below:**

There is a possibility that any person with an RFID reader can access the information being broadcasted. There arises a problem of uncertainty and unreliability when dealing with RFID cards and RFID technology. This is because any technology that can create a signal has the probability to be hacked. Usually, the RFID readers have small range. This range can be boosted by using boosters, but the system remains prone to the electromagnetic interference in amidst of electronic equipment. FID cards are very easily cloned. If someone has a handheld device such that it can read signals being broadcasted then they can clone the information using a transponder.

**Pioneers of RFID technology**

RFID technology is widely used technology in today’s market. There are many companies that are manufacturers of RFID tags and RFID readers. These companies have a huge monopoly among RFID technology-based product vendors. One of the largest manufacturers of UHF (ultra-high frequency) RFID readers is Motorola. Other manufacturers are CAEN RIFD, Impinj, Mojix, Alien Technology, Applied Wireless RFID, and GAO RFID. RFID tag manufacturers include Metal craft I.D. Plates & Labels, wave trend, zebra and many more.

### How RFID Cognitive Attendance System Works?

The aim of this project is to design an RFID based security access control system using ESP 32, in which only authorised personnel are allowed access to the student database attendance marking system. The working of the project is explained here.

When the circuit is powered ON, the microcontroller will initially the step to Swipe the Card .

When the RFID Card or Tag is swiped against the RFID reader, it will detect the ID card and sends the unique card no. to the microcontroller via serial terminal.

With the help of suitable programming, we need to compare the received card no. with the numbers that are already stored in the microcontroller or any database like external memory unit.

If the received number is matched with the already stored number, then the microcontroller will display the name of the card holder on the webpage and activates the motor driver IC. As a result,a buzzer will get initialized if the system matches with the persons identity in the database and the attendance will get marked in the webpage. Is the user authentication is false then the buzzer will ring twice and nothing will happen to the web page.