Enhanced Hash-Based Image Steganography to Increase Data Integrity and Confidentiality

B.Phanindra Kumar[1] G.V.Kathyayeni[2] G.Satish Kumar[3] D.Ajay[4] B.Lahari Devi[5]

[1]Assistant Professor, Department of ECE, NRIIT, Agiripalli, AP

[2,3,4,5] UG student, Department of ECE, NRIIT, Agiripalli, AP

Abstract: In the current world, providing secure data with confidentiality and integrity has become a big challenge mainly in the networking field. In order to improve the security of these existing parameters, in this paper, we have proposed a methodology through which integrity of the data could be maintained and extended the existing steganography technique that can increase confidentiality and integrity by utilizing various encryption and decryption methods to provide a collective result. In this work, we have used AES128, SHA256, and Image Steganography Cryptographic Methods. In order to provide secure data before sending it to the end-user. In this approach, we have concatenated Encrypted plain text and Hash code in an Image. Even though if there are any attacks happened the attacker will get only a RAW message but not plain text. Our Observation can enhance further development in various research areas.

Keyword: Encryption, SHA256, AES128, Image Steganography, Confidentiality & Integrity, Cryptology.

I.INTRODUCTION

Encryption is a concept of hiding data and sending it to the network. What are we getting through encryption? We are attaining confidentiality through the network. But what if the attacker catches the CIPHER text and tries to Decrypt it. So, for this case, we have so many encryption techniques and they have been proved to be the strongest techniques. For example, let us take AES are proved to be the strongest technique and AES is proved to be not compromised so far. Now let us consider hashing algorithms, they are used for the integrity check and one of the widely used hash algorithms are SHA256 and SHA512. They have proved themselves and proved to be the strongest hash algorithms available so far.

So previously there is a technique where a plain text is passed into the Encryption algorithm and ciphertext is obtained and in the same way, plaintext is passed into the hash algorithm and the hash value is generated and both the cipher text and hash value are concatenated and passed to the side of the receiver. Steganography is a concept of data hiding and it used two ways to hide the data. One is LSB (Least Significant Bit) Steganography and 1VISB (Most Significant bit Steganography). In this process, the plain text is sent into the image, and the steganographic image is sent to the receiver's side.

This is also the most successful procedure to hide the data and attain confidentiality. But let us consider the situation where a steganographic image is sent to the receiver's side and the image is captured by the attacker and he performs steganalysis 1101 There may be a chance that the attacker can perform steganalysis and he may reach the plain text. So, there is a chance of data leak from the image. By considering the above situations we can combine method-1 and method-2 and perform a secure data transmission and integrity enhancement using image steganography integrated with a hash function, that means first we are passing the plain text into the Encryption passed into the hash algorithm and the hash value is obtained. Now these are combining the ciphertext and the hash value and sending it into the Steganographic algorithm and the output we are getting is a steganographic image.

This steganographic image is sent to the receiver's side and the decryption process is done. The main use of our way of implementing the steganography is if the attacker captured the image that is the output of our procedure, then he will start steganalysis and what he can find is some part of the hash message or some part of ciphertext but not both and there is no chance he can figure out the total message from the image so it is very useful for the secret transmission between two parties without knowing to the third person. hash function and hash algorithm are checked if both the hash codes are same then the message is not modified through the channel.

So, in this way we are going to implement the steganography in a new way. There are many fields in which the project is implemented and some of them are in military fields where to transmit the secure data and in hospitals where the details of the patient are transmitted through the patent image. So, this project is different when compared to the previous papers we have read and can enhance confidentiality and integrity the same time. The second module of our project will be the decryption part. Here we are the first decrypting the concatenated message which is the output from our first module. The concatenated message consists of two parts these are ciphertext from the plain message and the hash value of the message which we are encoding. The procedure in which the message somewhat different from the conventional procedure. while they will be decoding will be somewhat different from the procedure. While the normal procedure of decoding the message from the steganographic image is the same as what we are doing here but the decrypted message isn't the plain text the decoded image will result in the concatenated message which is the output of module one which we have done early in this module, we are decoding the image and the concatenated message will be sent to another file where the message will be processed and separated. Then the concatenated message will be separated into two forms they are ciphertext and hash value.

The ciphertext is then decoded and again sent into the hash finding file and from there the hash is obtained to the hash file. Then these both i.e., hash value which is obtained from the decoded plain text which is obtained in the decryption module and the hash value which is obtained from the plain text which is obtained from the encoding module. Then these two hash values will be checked and if both the hash values are the same then the message is not altered from the encryption side to the decryption side. so, by this procedure, another security feature is being achieved which is integrity to the message. That means the message which is sent from the sender side is not altered in between to the side of the receiver this is called integrity. In this project, we are achieving two security features those are confidentiality and integrity. This is the module for the decryption side and this module is used to decrypt the message and checking the integrity of the message.

II.LITERATURE SURVEY

Steganography is the science and art of secret communication between two sides that attempt to hide the content of the message. It is the science of embedding information into the cover image without causing a loss in the cover image after embedding. Steganography is the art and technology of writing hidden messages in such a manner that no person, apart from the sender and supposed recipient, suspects the lifestyles of the message. It is gaining huge attention these days as it does now not attract attention to its information's existence. In this paper, a comparison of two different techniques is given. The first technique used Least Significant Bit (LSB) with no encryption and no compression. In the second technique, the secret message is encrypted first then LSB technique is applied. Moreover, Discrete Cosine Transform (DCT) is used to transform the image into the frequency domain. The LSB algorithm is implemented in spatial domain in which the payload bits are inserted into the least significant bits of cover image to develop the stego-image while DCT algorithm is implemented in frequency domain in which the stego-image is transformed from spatial domain to the frequency domain and the payload bits are inserted into the frequency components of the cover image. The performance of these two techniques is evaluated on the basis of the parameters MSE and PSNR. [1].

The establishment of a secure communication between two communicating parties is becoming a difficult problem due to the likelihood of attacks and other unintentional changes during an active communication over an unsecured network. However, the security of secret information can be secured using either cryptography or steganography. Steganography refers to the practice of concealing a message (with no traceability) in a manner that it will make no meaning to anyone else except the intended recipient, while cryptography, on the other hand, refers to the art of converting a plaintext (message) into an unreadable format. Thus, steganography conceals the existence of a secret message while cryptography alters the message format itself. Both steganographic and cryptographic techniques are powerful and robust. In this paper, the major aim is to review several ways of combining steganographic and cryptographic techniques to achieve a hybrid system. Moreover, some of the differences between cryptographic and steganographic techniques were presented as well. [2] With the advent of the World Wide Web and the emergence of ecommerce applications and social networks, organizations across the world generate a large amount of data daily. Information security is the most extreme basic issue in guaranteeing safe transmission of data through the web. Also network security issues are now becoming important as society is moving towards digital information age. As more and more users connect to the internet it attracts a lot of cyber-attacks. Its required to protect computer and network security i.e. the critical issues. The pernicious hubs make an issue in the system. It can utilize the assets of different hubs and safeguard the assets of its own. In this paper we provide an overview on Network Security and various techniques through which Network Security can be enhanced i.e. Cryptography. [3]

III.PROPOSED METHODOLOGY

In this proposed system a secure graphical user interface (GUI) for encrypting the data before transmission to the network. Firstly, we are encrypting the plain text using an encryption algorithm like AES 128 bit. We get cipher text as output. we pass the same plain text to the hash algorithm. Using an SHA 256 algorithm we generate a unique message digest. The concatenated message of cipher text and a unique message digest of hash is passed to the steganography tool where it asks us to select an image to store the information and we get encrypted Steg Message by these we are enhancing the security where we are attaining confidentiality and integrity. Through our project, we are able to hide data in an efficient way and can also transmit the data in the form of an image. And also, we are achieving all this by creating a single application and hide the data securely and safely into the image. So, in this way the integrity and confidentiality of an image is enhanced.

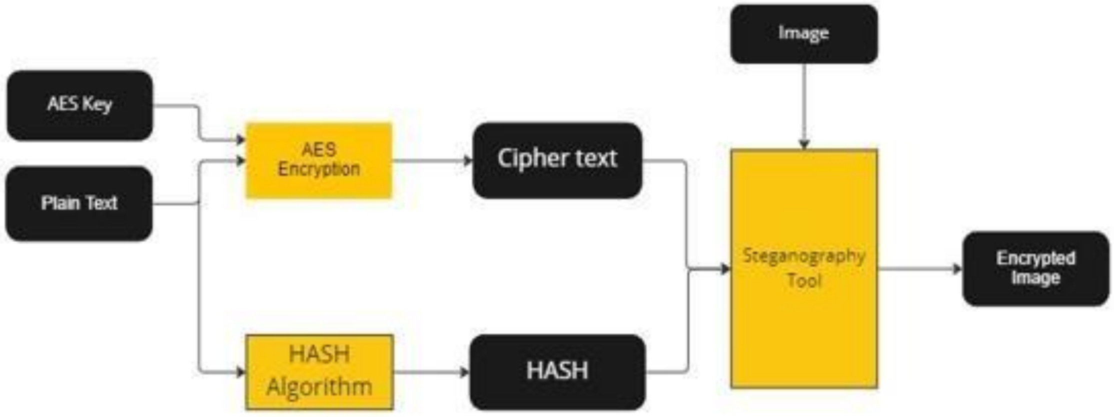


Fig1: BLOCK DIAGRAM FOR ENCRYPTION PART OF PLAIN TEXT USING IMAGE STEGANOGRAPHY

The above block diagram how we are enhancing the integrity of data by using the encryption algorithms. The first block specifies the plain text and the key passes through an encryption algorithm of Advanced Encryption Standard 128-bit and we are generating the cipher text. The plain text again passes through the hash algorithm of SHA 256 and generates a unique message digest. The second block specifies the concatenated message of cipher text and a unique message digest. The concatenated message passes through a steganographic tool with an image.

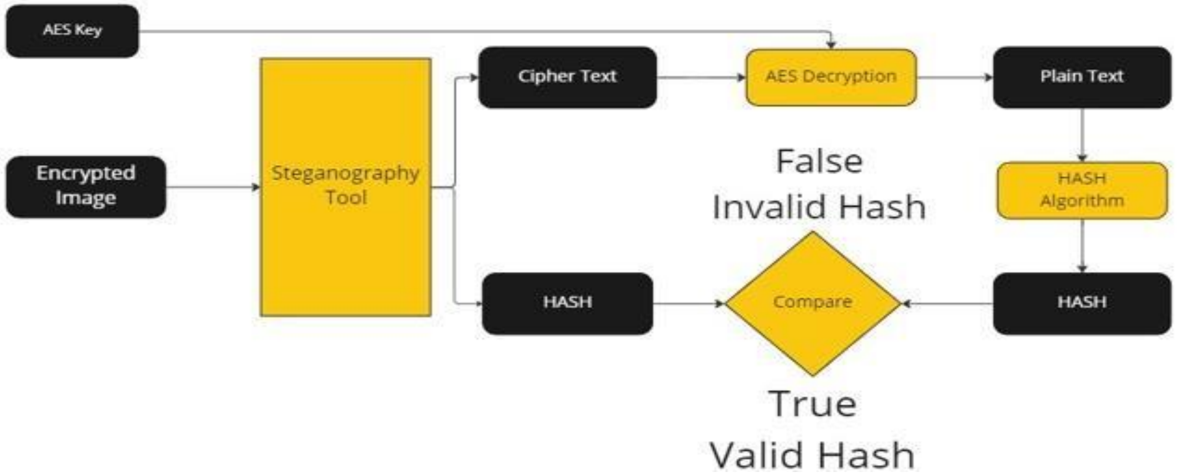


Fig2: BLOCK DIAGRAM FOR DECRYPTION PART OF ENCRYPTED IMAGE USING IMAGE STEGNOGRAPHY

The steganographic generated the binary code of the concatenated message. The output specifies an encrypted image in which the binary representation of data is embedded. From the above diagram, using steganography the image will be decoded the image and the concatenated message will be sent to another file where the message will be processed and separated. Then the concatenated message will be separated into two forms they are ciphertext and hash value. The ciphertext is then decoded and again sent into the hash finding file and from there the hash is obtained to the hash file.

Block Diagram

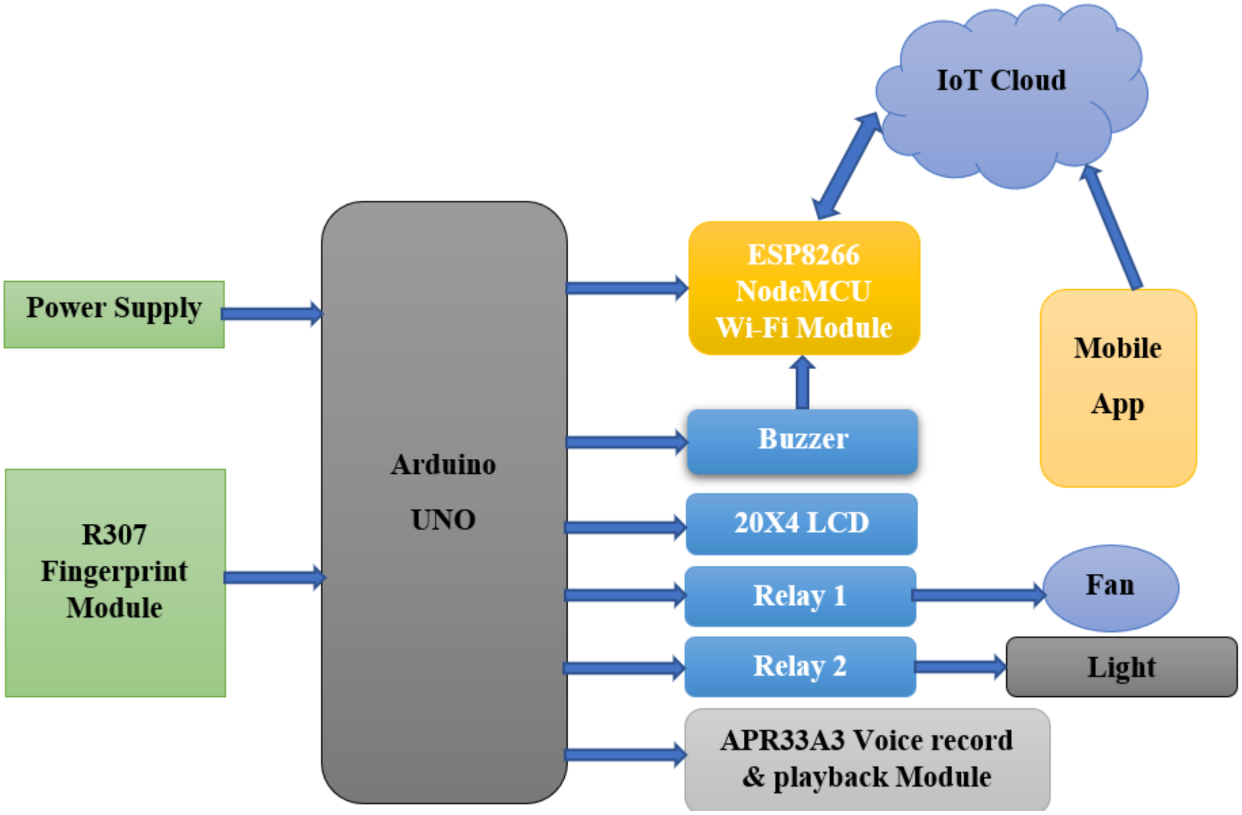


Fig1: Block diagram of Smart Classroom

a) Arduino UNO:

Arduino UNO is a microcontroller board based on the ATmega328P. It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz ceramic resonator, a USB connection, a power jack, an ICSP header and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with an AC-to-DC adapter or battery to get started. Arduino is an open-source electronics platform based on easy-to-use hardware and software. Arduino boards can read inputs - light on a sensor, a finger on a button, or a Twitter message - and turn it into an output - activating a motor, turning on an LED, publishing something online.

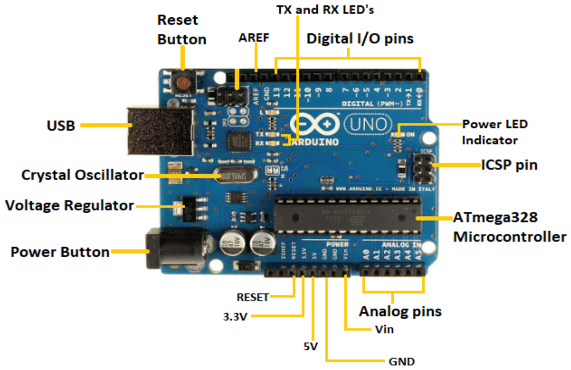


Fig3: Arduino UNO

b) ESP8266 Wi-Fi module:

In 2014, an ESP8266 Wi-Fi module was introduced and developed by third-party manufacturers like AI thinkers, which is mainly utilized for IoT-based embedded applications development. It is capable of handling various functions of the Wi-Fi network from another application processor. It is a SOC integrated with a TCP/IP protocol stack, which can provide microcontroller access to any type of Wi-Fi network. This article deals with the pin configuration, specifications, circuit diagram, applications, and alternatives of the ESP8266 Wi-Fi module.

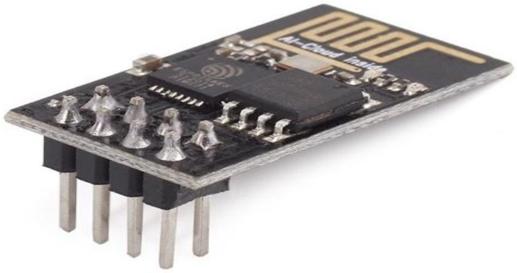


Fig4: ESP8266 Wi-Fi Module

c) R307 Fingerprint Module:

R307 Fingerprint Module consists of optical fingerprint sensor, high-speed DSP processor, high-performance fingerprint alignment algorithm, high-capacity FLASH chips and other hardware and software composition, stable performance, simple structure, with fingerprint entry, image processing, fingerprint matching, search and template storage and other functions.

Fig5: R307 Fingerprint Module

d) APR33A3 Voice Playback Module:

APR33A3 module provides high quality audio record and playback up to 11 minutes with 8 Khz sampling rate and 16-bit resolution. Using on board jumpers total duration can be divided into 1,2,4,8 messages which can be triggered by onboard switches or external triggers using external microcontroller pins.

Fig6: APR33A3 Voice Playback Module

e) Relay Board:

The four-channel relay module contains four 5V relays and the associated switching and isolating components, which makes interfacing with a microcontroller or sensor easy with minimum components and connections. The contacts on each relay are specified for 250VAC and30VDC and 10A in each case, as marked on the body of the relays.

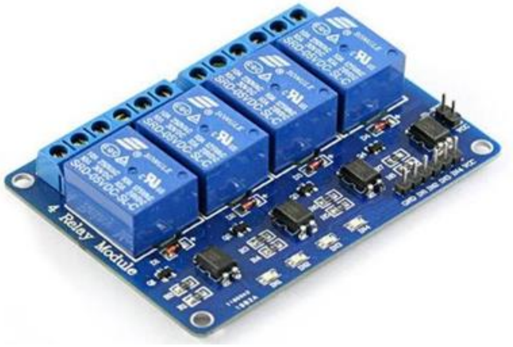


Fig7: Relay Board

IV.IMPLEMENTATION AND WORKING

In the design of MIT App Inventor, introducing mobile app development in educational contexts was a central goal. Prior to its release, most development environments for mobile applications were clunky, only accessible with expertise in systems level or embedded programming, or both. Even with Google's Android operating system and the Java programming language, designing the user interface was a complex task. Further, use of the platform required familiarity with Java syntax and semantics, and the ability to debug Java compilation errors (e.g., misspelled variables or misplaced semicolons) for success. These challenges presented barriers to entry for individuals not versed in computer science, App Inventor's target demographic. We briefly highlight and discuss design goals for the App Inventor project, specifically, the use of components to abstract some of the complexity of platform behavior, and the use of blocks to eliminate complexity of the underlying programming language. These goals can be further explained as aligning the visual language to the mental models of young developers and enabling exploration through fast, iterative design.

FLOW CHART:

Initialize the variables with the Voice announcement, Fingerprint Module, and any important notices. From the voice announcement step, it goes to attendance processing and after fingerprint module is activated, speaker functioning will be enabled. After attendance processing and important notices will be displayed in the LCD screen. The attendance that was processed will also go to the Excel sheet. Hence, this is the functioning of entire project.

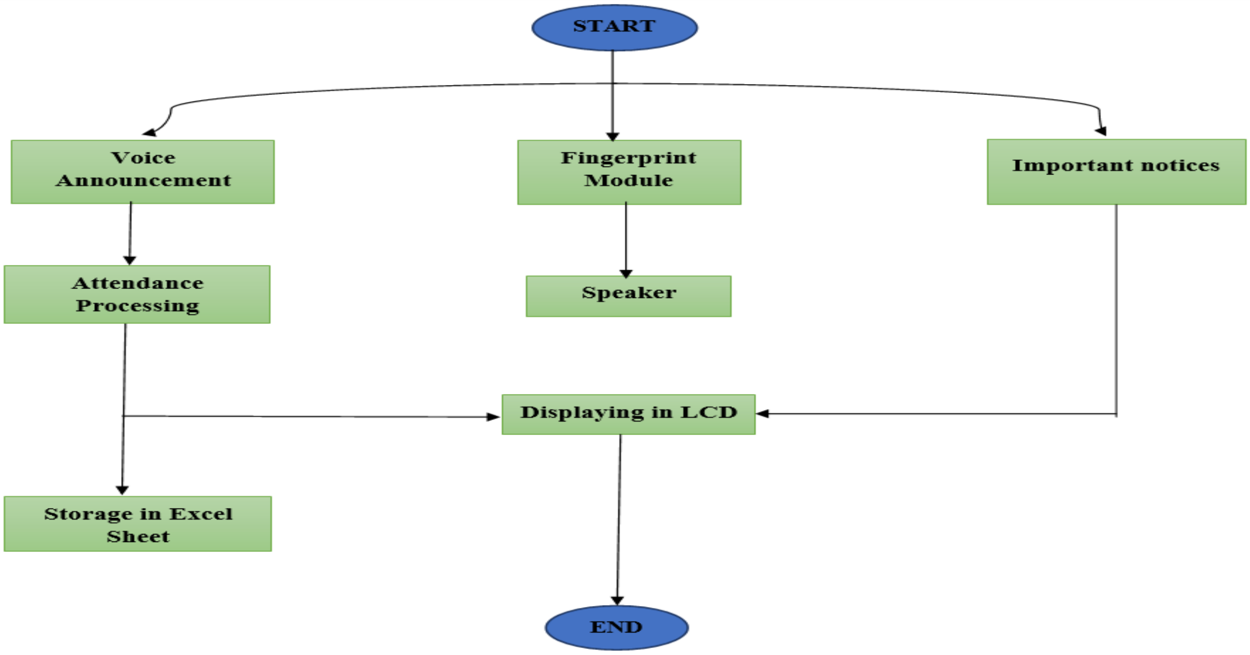


Fig8: Flow chart

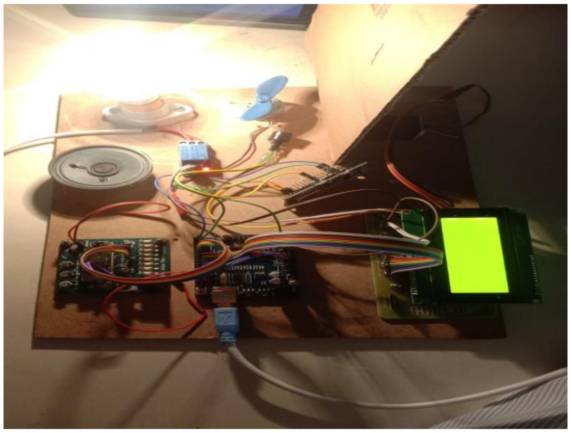
IV.RESULTS

a. Speaker

b. LCD displaying "Scan Thumb"

c. After the finger is placed on the scanner

d. Notice displayed in LCD



e. Functioning of Light.

f. Functioning of Fan

V. CONCLUSION AND FUTURE SCOPE

Our proposed Smart classroom increases the precision of work and reduces the man work. Due to its economic cost it can be easily implemented in every class room. By digitalizing those system, better infrastructure can be achieved and chances of errors are nulled. In Future, wireless Shield can be interfaced with Arduino microcontroller to stream presentation from mobile phones and tablets to the display devices like projector.

The Attendance system using face recognition can be developed in future. The Infrastructure can be developed.

REFERENCE

[1] Jungwoo Lee, "Smart classroom: Converging Smart technologies, Novel Content and advanced Pedagogies for future of

Education", Journal of Education and Vocational Research ISSN 2221 – 2590 Volume 4, Number 1, pp.5-9, Jan 2013.

[2] Unnati A. Patel, "Student Management System based on RFID Technology", International Journal of Emerging Trends & Technology in Computer Science. (IJETTCS) Volume 2, Issue 6, November – December 2013.

[3] Nivetha.S.R, "SMS based Wireless Notice Board with monitoring system", International Journal of Advanced Electrical and Electronics Engineering (IJAEEE) ISSN (Print) : 2278-8948, Volume 2, Issue 3, 2013

[4] Baoping Li, "Development and validation of the smart classroom inventory", SpringerOpen journal DOI 10.1186/s40561-015-0012-0.

[5] Abowd, G.D, "an experiment with the instrumentation of living education environment IBM system", Journal Volume 38, Number 4, 508-530.

[6] Das, S.K. and Cook, D.J, "Designing and modelling smart environments Proceedings of world of wireless, mobile and multimedia networks", WoWMoM 5 pp.

[7] Davar Pishva, "Smart classroom for Distance Education and their adoption to multiple classroom Architecture", Journal of Network Volume 3, Number 5, May 2008.

[8] Anik Barua, "Embedded System: Security Threats and Solutions", American Journal of Engineering Research (AJER) eISSN: 2320-0847 p-ISSN: 2320- 0936 Volume 3, Issue 12, pp-119-123.