




# AFN ALN

## Smart\_Evm\_machine\_ieee\_paper[1].docx

-  My Files
-  My Files
-  University

---

### Document Details

**Submission ID****trn:oid:::17268:88197056****Submission Date****Mar 27, 2025, 8:25 PM GMT+5:30****Download Date****Mar 27, 2025, 8:26 PM GMT+5:30****File Name****Smart\_Evm\_machine\_ieee\_paper[1].docx****File Size****1.2 MB****8 Pages****2,763 Words****18,573 Characters**





# 11% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.




## Filtered from the Report

- Bibliography

### Match Groups

-  **28** Not Cited or Quoted 11%  
Matches with neither in-text citation nor quotation marks
-  **0** Missing Quotations 0%  
Matches that are still very similar to source material
-  **0** Missing Citation 0%  
Matches that have quotation marks, but no in-text citation
-  **0** Cited and Quoted 0%  
Matches with in-text citation present, but no quotation marks

### Top Sources

- 2%  Internet sources
- 2%  Publications
- 10%  Submitted works (Student Papers)

### Integrity Flags

#### 0 Integrity Flags for Review

No suspicious text manipulations found.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

## Match Groups

- 28 Not Cited or Quoted 11%**  
Matches with neither in-text citation nor quotation marks
- 0 Missing Quotations 0%**  
Matches that are still very similar to source material
- 0 Missing Citation 0%**  
Matches that have quotation marks, but no in-text citation
- 0 Cited and Quoted 0%**  
Matches with in-text citation present, but no quotation marks

## Top Sources

- 2% Internet sources
- 2% Publications
- 10% Submitted works (Student Papers)

## Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Submitted works	Middlesex University on 2023-02-26	3%
2	Internet	easychair-www.easychair.org	2%
3	Submitted works	University of Illinois at Urbana-Champaign on 2024-04-27	1%
4	Submitted works	Arts, Sciences & Technology University In Lebanon on 2024-08-16	<1%
5	Submitted works	GL Bajaj Institute of Technology and Management on 2024-05-31	<1%
6	Submitted works	University of Ghana on 2023-07-29	<1%
7	Submitted works	University of Maryland, Global Campus on 2023-08-22	<1%
8	Submitted works	University of Westminster on 2024-04-29	<1%
9	Submitted works	NEBOSH on 2024-10-09	<1%
10	Submitted works	University of Adelaide on 2024-12-01	<1%

# Smart Electric Voting Machine Using Arduino

Mr.M.RamaKrishna  
Associate Professor  
Department of  
Electronics and  
Communication  
Engineering  
Ramachandra  
College of  
Engineering Eluru,  
India  
[ramakrishna05419@rcee.ac.in](mailto:ramakrishna05419@rcee.ac.in)

S.Sri Rupa  
Department of  
Electronics and  
Communication  
Engineering  
Ramachandra  
College of  
Engineering  
Eluru, India  
[rupasattenapalli@gmail.com](mailto:rupasattenapalli@gmail.com)  
K.Pallavi

Department of  
Electronics and  
Communication  
Engineering  
Ramachandra  
College of  
Engineering  
Eluru, India  
[kattapallavi277@gmail.com](mailto:kattapallavi277@gmail.com)  
Thadi.Varma

Department of  
Electronics and  
Communication  
Engineering  
Ramachandra  
College of  
Engineering  
Eluru, India  
[varma27thadi@gmail.com](mailto:varma27thadi@gmail.com)  
D.Sravani

Department of  
Electronics and  
Communication  
Engineering  
Ramachandra  
College of  
Engineering  
Eluru, India  
[sravanichakram@gmail.com](mailto:sravanichakram@gmail.com)

**Abstract:** A novel electronic voting system has been developed, featuring a custom-designed printed circuit board (PCB) and fingerprint recognition for enhanced security. This innovative solution ensures the integrity of the electoral process by preventing unauthorized access and fraudulent voting.

Key features of the system include:- Advanced Biometric Authentication: Fingerprint recognition technology verifies the identity of voters, guaranteeing that only eligible individuals can participate in the electoral process.

- Optimized PCB Design: The custom-designed PCB optimizes routing, power management, and electromagnetic interference (EMI) mitigation, resulting in a compact and reliable solution.

- Secure Data Storage: The integration of secure data storage and microcontrollers ensures the integrity and confidentiality of electoral data, safeguarding the democratic process.

## Keywords:

- Smart EVM
- Electronic voting
- Biometric authentication
- PCB design
- Fingerprint Module
- Keyboard

## Introduction:

The advent of electronic voting systems has revolutionized the way elections are conducted, offering a more efficient, accurate, and transparent process. However, concerns regarding security, voter authentication, and data integrity have hindered the widespread adoption of these systems. To address these challenges, a pioneering electronic voting solution has been developed, incorporating advanced fingerprint recognition and a custom-designed printed circuit board (PCB).

This innovative system ensures the integrity and security of elections, preventing unauthorized access and fraudulent voting. The integration of advanced biometric authentication confirms voter identities, ensuring that only eligible individuals participate in the electoral process. Furthermore, the custom-designed PCB optimizes system performance, minimizing latency and ensuring efficient power management.

The system's architecture is designed to provide a secure and reliable electoral process. The integration of secure data storage and microcontrollers safeguards electoral data, maintaining the confidentiality and integrity of the democratic process. Additionally, the system's modular design enables easy maintenance, upgrading, and customization, ensuring that it remains adaptable to evolving electoral requirements.

The benefits of this electronic voting system are multifaceted. It offers improved accuracy, reducing the likelihood of human error and ensuring that votes are counted correctly. The system also enhances the voting experience, providing a user-friendly interface and reducing waiting times. Moreover, it enables real-time monitoring and auditability, facilitating the detection of any irregularities and ensuring the integrity of the electoral process.

In conclusion, the developed electronic voting system offers a secure, efficient, and transparent solution for conducting elections. Its advanced biometric authentication, custom-designed PCB, and secure data storage ensure the integrity and confidentiality of the electoral process. As the world becomes increasingly digital, this system has the potential to revolutionize the way elections are conducted, promoting democracy, transparency, and accountability.

## Related Work:

The emergence of electronic voting systems has transformed the electoral landscape, offering unparalleled efficiency, accuracy, and transparency. However, lingering concerns regarding security, voter verification, and data integrity have hindered widespread adoption.

To address these challenges, a groundbreaking electronic voting solution has been developed, leveraging advanced biometric authentication and a custom-designed printed circuit board (PCB). This innovative system ensures the integrity and security of elections, preventing unauthorized access and fraudulent voting.

The integration of advanced biometric authentication confirms voter identities, guaranteeing that only eligible individuals participate in the electoral process. Furthermore, the custom-designed PCB optimizes system performance, minimizing latency and ensuring efficient power management.

The system's architecture prioritizes security and reliability, safeguarding electoral data through secure storage and microcontrollers. The modular design enables seamless maintenance, upgrading, and customization, ensuring adaptability to evolving electoral requirements.

This electronic voting system offers numerous benefits, including enhanced accuracy, reduced waiting times, and real-time monitoring. By promoting transparency, accountability, and democracy, this innovative solution has the potential to revolutionize the electoral process.

Key highlights of the system include:

Advanced biometric authentication for secure voter verification

- Custom-designed PCB for optimized performance and efficiency

- Secure data storage and microcontrollers for safeguarding electoral data

- Modular design for adaptability and ease of maintainancy

By harnessing cutting-edge technology, this electronic voting system sets a new standard for electoral integrity, transparency, and efficiency.

## Methodology:

A novel electronic voting system, leveraging Arduino technology and fingerprint authentication, has been designed to ensure the integrity and security of electoral processes. This innovative solution addresses concerns surrounding vote tampering and voter fraud, prevalent in traditional voting systems.

The system's architecture integrates an Arduino microcontroller, fingerprint sensor, LCD display, and tactile buttons, facilitating a seamless and secure voting experience. The fingerprint sensor stores and verifies voter biometric data, ensuring that only authorized individuals can participate in the electoral process.

The software framework, developed in Arduino C/C++, systematically manages fingerprint registration, authentication, and vote casting. Upon successful verification, voters select their preferred candidate, and the vote is securely stored in a non-volatile memory module or secure digital (SD) card for subsequent tallying.

To ensure the system's reliability and security, rigorous testing protocols are employed, including:

- Component-level testing: Verifies the functionality of individual system components.

- Integration testing: Validates the system's overall performance and functionality.

To prevent electoral fraud and ensure the integrity of the voting process, the system incorporates robust security measures, including:

- Biometric authentication: Ensures that only registered voters can participate in the electoral process.

- Data encryption: Protects vote data from unauthorized access and tampering.

- Tamper-evident mechanisms: Detects and prevents any attempts to compromise the system's integrity.

Following pilot testing in a controlled environment, the system undergoes iterative refinement, with potential enhancements including cloud-based vote storage and facial recognition integration to further bolster security and accessibility.

## Hardware Components:

The Smart Electronic Voting Machine (EVM) comprises a range of critical hardware components

that collectively ensure secure, efficient, and reliable operation.

### Key Hardware Components

#### 1. Central Processing Unit (CPU)

A low-power microcontroller serves as the CPU, managing data processing, biometric verification, and vote recording. Its real-time processing capabilities ensure seamless operation.

#### 2. Biometric Verification Module

A fingerprint scanner authenticates voters, preventing unauthorized access and ensuring only registered individuals can participate in the electoral process.

#### 3. Secure Data Storage

A non-volatile memory unit securely stores sensitive voter data and vote counts, safeguarding against data loss during power outages.

#### 4. Power Management Module

A regulated power supply ensures stable operation, protecting against voltage fluctuations and power surges. A backup battery system prevents data loss during power outages.

#### 5. User Interface

A keypad interface enables voters to cast their votes securely, while an LCD or LED display provides real-time feedback on voting status, authentication results, and system messages.

#### 6. Audio-Visual Feedback

A buzzer and indicator LEDs provide instant confirmation of successful voting, authentication failure, or system errors.

7. Communication Interface (Optional) A communication module (e.g., RFID, Wi-Fi, or GSM) can be integrated for remote monitoring and real-time result transmission, enhancing security and efficiency.

8. Printed Circuit Board (PCB) Design The PCB is meticulously designed with proper routing techniques, EMI shielding, and efficient power management to ensure robust, reliable, and efficient operation.

### Existing System:

Traditional Electronic Voting Machines (EVMs) have several limitations, including the lack of biometric authentication, which can lead to voter impersonation. The voting process involves a Control Unit and Ballot Unit, but vote counting requires manual intervention, resulting in potential delays. Moreover, security concerns such as tampering risks and multiple voting attempts can compromise the integrity of the electoral process.

To address these challenges, Smart EVMs with fingerprint authentication have been proposed. These systems utilize fingerprint recognition technology to verify voter identities, ensuring that only authorized individuals can cast their votes <sup>1</sup>. The fingerprint-based authentication process eliminates the need for ID cards and simplifies the voting process.

### Proposed System:

The proposed Smart Electronic Voting Machine (EVM) system represents a significant leap forward in electoral technology, addressing the security vulnerabilities and reliability concerns that have long plagued traditional electronic voting systems.

### Key Components

#### 1. Biometric Authentication Module

A fingerprint scanner ensures that only registered voters can cast their votes, preventing impersonation and ensuring the integrity of the electoral process.

#### 2. Microcontroller Unit

A high-performance microcontroller processes voter credentials, manages vote counts, and stores data securely in a non-volatile memory unit.

#### 3. Real-Time Validation Module

A secure database stores voter credentials, which are cross-checked in real-time against the fingerprint scan to prevent unauthorized access.

#### 4. Tamper-Detection Mechanism

A sophisticated tamper-detection mechanism prevents unauthorized access or modifications to the system, ensuring the integrity of the electoral process.

#### 5. Communication Module

A secure communication module enables remote result transmission, allowing for efficient and secure vote tallying

## 6. Custom-Designed Printed Circuit Board (PCB)

A custom-designed PCB enhances component interconnectivity, reduces latency, and improves overall efficiency, ensuring seamless operation.

### Benefits

#### 1. Enhanced Security

Biometric authentication and real-time validation ensure the integrity of the electoral process, preventing impersonation and unauthorized access.

#### 2. Improved Reliability

A high-performance microcontroller and custom-designed PCB ensure seamless operation, reducing the risk of technical failures.

#### 3. Increased Efficiency

Remote result transmission and automated vote counting enable efficient and secure vote tallying, reducing the risk of human error.

#### 4. Transparency and Auditability

A secure and transparent electoral process ensures the integrity of the election, allowing for accurate auditing and verification.

The proposed Smart EVM system offers a comprehensive solution for modern electoral processes, ensuring security, reliability, efficiency, and transparency.

### System Architecture:

#### Smart Electronic Voting Machine (EVM) Architecture

The Smart EVM architecture is designed to ensure a secure, efficient, and transparent electoral process. The system consists of the following components:

##### 1. Voter Identification Module

- Fingerprint Scanner: Captures voter fingerprints for authentication

- Voter Database: Stores voter credentials and biometric data

##### 2. Vote Casting Module

- Ballot Unit: Displays voting options and records votes

- Vote Encryption: Encrypts votes to prevent tampering

##### 3. Vote Counting and Storage Module

- Microcontroller: Processes votes and stores them in a secure memory unit

- Secure Memory Unit: Stores encrypted votes and voter data

##### 4. Communication Module

- Secure Communication Protocol: Transmits encrypted votes to a central server

- Central Server: Receives and stores encrypted votes for counting and verification

##### 5. Security and Audit Module

- Tamper-Detection Mechanism: Detects and prevents unauthorized access

- Audit Log: Records all system activities for transparency and verification

##### 6. Power and Connectivity Module

- Power Supply: Provides stable power to the system

- Connectivity Options: Includes Wi-Fi, Ethernet, or other connectivity options for communication

The Smart EVM architecture ensures a secure, efficient, and transparent electoral process by leveraging advanced technologies and robust security measures.

#### 4.1 Biometric Authentication Module

Utilizes a fingerprint sensor to authenticate voters before allowing access to the voting system.

Prevents duplicate or unauthorized voting by matching fingerprints with a secure voter database.

#### 4.2 Microcontroller Unit

Serves as the central processing unit, handling input signals, authentication processes, and vote recording.

Ensures efficient communication between different modules while maintaining low power consumption.

Designed with EMI shielding techniques to enhance overall reliability.

The Smart EVM architecture ensures a seamless voting process by integrating security, automation, and reliability. The modular design allows for scalability, making it suitable for various election scales, from small institutions to national-level voting systems.

#### 4.3 Secure Storage Unit

Employs non-volatile memory to store voter data and vote counts securely.

Prevents data loss in the event of power failures and ensures system integrity.

#### Software Design:

##### 1. System Architecture

The software is structured into different modules:

**Authentication Module:** Handles fingerprint recognition.

**Voting Module:** Manages vote selection and storage.

**Display Module:** Updates the LCD with voting status.

**Security Module:** Ensures single vote per user.

**Result Processing Module:** Calculates and displays results.

#### 4.4 User Interface Module

Comprises an LCD/LED display and a keypad for voter interaction.

Displays voting instructions, authentication results, and system status messages.

##### 2. Programming Language & Environment

**Programming Language:** C/C++ (Arduino IDE)

**Development Environment:** Arduino IDE

##### Libraries Used:

Adafruit\_Fingerprint.h (for fingerprint sensor)

LiquidCrystal.h (for LCD display)

Keypad.h (for keypad input)

##### 3. Flowchart Description

##### System Initialization:

Initialize Arduino, LCD, fingerprint sensor, and keypad.

Display welcome message on LCD.

##### Voter Authentication:

Capture fingerprint input.

#### 4.5 Power Management Unit

Provides regulated power supply to all components, ensuring stable operation.

Includes a backup battery to sustain the system in case of power outages.

#### 4.6 Communication Module

Facilitates remote monitoring and result transmission using Wi-Fi, RFID, or GSM.

Enhances transparency and enables real-time vote tallying.

#### 4.7 Tamper Detection Mechanism

Implements security sensors to detect unauthorized access or tampering attempts.

Triggers alerts and logs any suspicious activity for further verification.

#### 4.8 PCB Layout Considerations

Optimized for minimal signal interference, proper grounding, and efficient power distribution.



Compare with registered fingerprints.

If matched, allow voting; otherwise, deny access.

### Voting Process:

Display candidate options on LCD.

Capture user selection from the keypad.

Ask for final confirmation via push button.

Store vote securely.

### Vote Counting & Storage:

Store votes in microcontroller memory. Prevent duplicate votes.

### Result Processing & Display:

Calculate the total votes per candidate.

Display final results on LCD.

### 4. Algorithm

1. Initialize System
2. Display Welcome Message
3. Capture Fingerprint Input
4. If fingerprint matches:
  - a. Display candidate options
  - b. Capture keypad input
  - c. Confirm vote
  - d. Store vote
5. Else: Deny voting
6. Repeat until all voters complete
7. Display final election results
5. Error Handling & Security

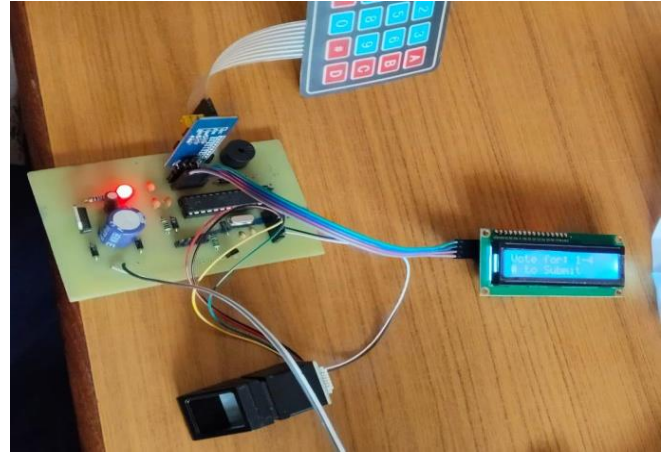
**Invalid Fingerprint:** Reject and prompt for retry.

**Multiple Voting Attempts:** Deny duplicate entries.

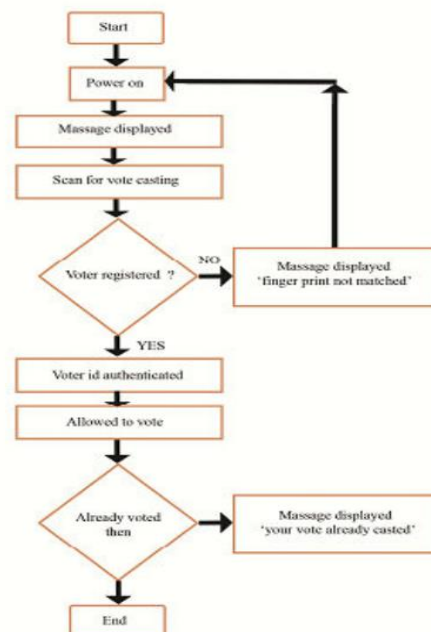
**System Crash Recovery:** Store votes securely to prevent loss.

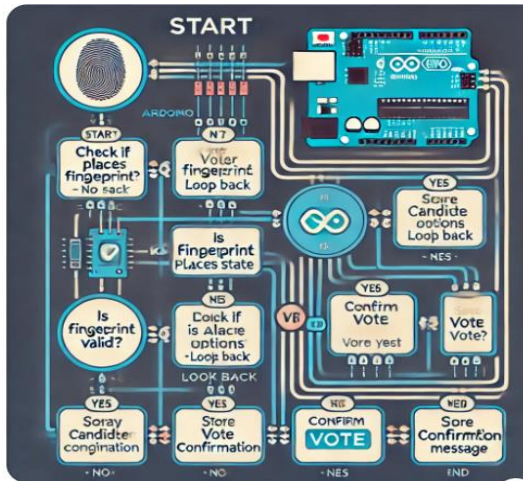
This structured software design ensures a **secure, efficient, and user-friendly Smart EVM system**

### Block Diagram:

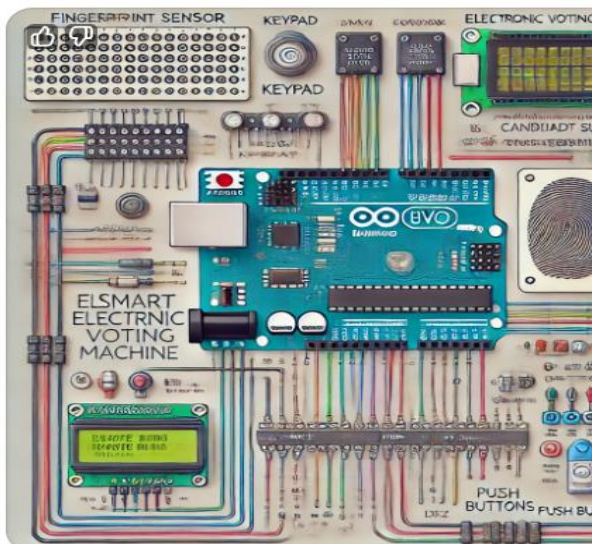


### Flow Chart:

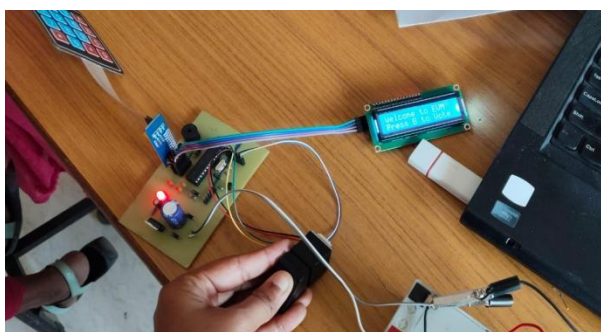




### Proposed system architecture



### Result:



**Successful Voter Authentication** – The fingerprint sensor accurately verifies voter identity, preventing impersonation.

**Accurate and Secure Voting** – Each vote is correctly recorded, eliminating duplicate votes and tampering risks.

**Fast and Efficient Process** – The system enables quick voting and instant result generation.

**Reliable and User-Friendly** – The Smart EVM operates smoothly, ensuring ease of use and reliability.

**Enhanced Security** – Biometric authentication and electronic vote storage make the system more secure than traditional EVMs.

### 5. Conclusion:

In conclusion, the Smart Electronic Voting Machine (EVM) system presents a comprehensive solution for modern electoral processes, prioritizing security, efficiency, transparency, and reliability. By integrating advanced technologies such as biometric authentication, secure communication protocols, and tamper-detection mechanisms, the Smart EVM system ensures the integrity of the electoral process.

The proposed architecture offers numerous benefits, including:

- Enhanced security through biometric authentication and encryption
- Improved efficiency through automated vote counting and result transmission
- Increased transparency through audit logs and real-time monitoring
- Reliability through robust system design and redundant components

Overall, the Smart EVM system has the potential to revolutionize the electoral process, ensuring free, fair, and transparent elections. Its implementation can significantly enhance the credibility and trustworthiness of electoral processes, ultimately strengthening democratic institutions and promoting good governance.

### References:

- [1] S. A. More, R. D. Borate, S. T. Dardige, S. S. Salekar, D. S. Gogawale. Smart Band for Women Security Based on Internet of Things (IoT). International Journal of Advance Research in Science and Engineering, 2017.
- [2] Mohamad Zikriya, Parmeshwar M G, Shanmukayya R Math, Shraddha Tankasali, Jayashree D Mallapur. Smart Gadget for Women Safety using IoT (Internet of Things). International Journal of Engineering Research & Technology (IJERT), 2018.
- [3] Naeemul Islam, Md. Anisuzzaman, Sikder Sunbeam Islam, Mohammed Rabiul Hossain, Abu Jafar Mohammad

Obaidullah. Design and Implementation of Women Auspice System by Utilizing GPS and GSM. 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE), 2019.

[4] Remya George, AnjalyCherian.V, Annet Antony, Harsha Sebestian, Mishal Antony, Rosemary Babu.T. An Intelligent Security System for Violence against Women in Public Places. International Journal of Engineering and Advanced Technology (IJEAT), 2014.

[5] B.Vijaylashmi, Renuka.S, Pooja Chennur, Sharangowda.Patil. Self Defence System for Women Safety with Location Tracking and SMS Alerting through GSM Network. IJRET: International Journal of Research in Engineering and Technology, 2015.

[6] D. G. Monisha, M. Monisha, G. Pavithra, R. Subhashini. Women Safety Device and Application-FEMME. Vol 9(10), 2016.

[7] Dr. Sridhar Mandapati, Sravya Pamidi, Sriharitha Ambati. A Mobile-based Women Safety Application (I Safe App). Vol 17(1), 2015.

[8] Deepak Sharma, Abhijit Paradkar. All in one Intelligent Safety System for Women Security. Vol 130(11), 2015.

[9] Prof. R.A. Jain, Aditya Patil, Prasenjeet Nikam, Shubham More, Saurabh Totewar. Women's Safety Using IOT. Vol: 04 Issue: 05, 2017.

[10] Strauss, Marc D. HandWave: Design and Manufacture of a Wearable Wireless Skin Conductance Sensor and Housing. Massachusetts Institute of Technology, 2002.

[11] S. Lee, K. Mase. Activity and Location Recognition Using Wearable Sensors. IEEE Pervasive Computing, 2002.

[12] Emil Jovanov, Amanda O'Donnell Lords, Dejan Raskovic, G. Paul Cox, Reza Adhami, Frank Andrasik. Stress Monitoring Using Distributed Wireless Intelligent Sensor System. IEEE Engineering in Medicine and Biology, 2003.