Design and Implementation of a Software-Based Advance Electronic Voting Machine Using Automatic Registration and Fingerprint Identification

Jehangir Arshad (Jehangirarshad@cuilahore.edu.pk)
COMSATS University Islamabad Lahore Campus
Muhammad Farooq-i-Azam
COMSATS University Islamabad Lahore Campus
Ayesha Khan
COMSATS University Islamabad Lahore Campus https://orcid.org/0000-0003-0243-8340
Muhammad Irshad
The Hong Kong Polytechnic University
Sohail M. Noman
Shantou University Medical College

Research Article

Keywords: Electronic Voting Machine (EVM), Automatic Registration, Fingerprint Identification, Secure Socket Layer (SSL), MYSQL Server

Posted Date: August 10th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-762430/v1

Abstract

In democratic countries, free and fair elections are required to quantify the populace's sentiments to form a government of representatives. It is challenging to maneuver due to the procedural variation from country to country and complexity. As paper-based electoral systems are slow and prone to error that take hours and ample manpower to announce the results, thus a secure efficient electoral system is always preferred. In this paper, we have proposed a secure implementation of auto-registration fingerprint identification-based electronic voting systems to overcome the aspect of accuracy and transparency. We have included a novel feature of automated registration to authenticate the user through identity before the vote casting. Moreover, credentials of voters are collected in a database including fingerprints, and communication of encrypted data between server and machine with secured Secure Socket Layer (SSL). Additionally, the voter can cast their votes through a touch screen Graphical User Interface (GUI), and once the voting time end, the screen can automatically disappear by authorizing admin to print Form-45. Conclusively, the proposed system count votes automatically that is much faster and accurate than the traditional voting techniques. Moreover, the results will be available to the general public in 1-2 hours which ensures fair elections.

1. Introduction

Elections are crucial in our democratic country because they allow citizens to choose a government leader. The world's voting system has been riddled with numerous fundamental flaws, resulting in a corrupt candidate winning an election. The election malpractices observed at various levels of electing a representative have caused researchers to be emotionally, physically, socially, and intellectually concerned. Using a traditional election system to collect votes from citizens is no longer considered efficient due to unreliability (Shahzad, 2019)- (Yang, 2018). The paper-based voting system is the traditional style of voting that contains many disadvantages. As technology is advanced, we need to update our voting system to improve reliability, trust, and convenience. For this purpose, the electronic voting system was introduced. The electronic voting system is also known as e-voting. It is a voting procedure that uses electronic means to take care of casting and counting votes (Srikrishnaswetha, 2019)- (Yi, 2013).

In 2000, Optical scan voting systems were used for counting elections using the Data Reduction software (DRS) to cover documents, process integration e-form capture, and document retrieval) plc of Milton Keynes in London. In 2004, Optical character recognition (OCR) is an electronically identify the printed characters or photos using computer software or photoelectric devices) were used to scan and processed assembly and European parliamentary elections of London Mayoral (Kumar, 2012). In 2007, the Scottish council and parliament general elections were used an optical scan voting system to count paper ballots electronically. After counting, UK electoral commission generated a report of errors in voting procedure there were more than 150,000 votes are invalid or spoilt. So, 56000 list ballots and 86000 constituency ballots were rejected. Due to the reason that voters have to cast vote for both sections on a single ballot

paper. Due to this reason Scottish parliamentary and council elections were used different electronic techniques for their voting system (Mithe, 2013).

Many different countries are using different types of electronic machines for their voting process. The Election Commission of Dhaka recently presented security features to the tribunes of DHAKA and provided information on the use of Electronic Voting Machines. The Election Commission of DHAKA claims that the Electronic Voting Machine is impossible to hack because of its multiple layers of security (Irani, 2018)- (Nair, 2015). In 2014, Virendar Kumar Yadav presented a study on Electronic Voting System using UIdAI (Unique Identification Authority of India), It is a Governmental agency of India which assigns a unique 12-digit identity number to each voter. In this paper, they presented a study about an approach towards an Electronic Voting system that ensures authentication, authorization, and accounting using UIDAI. In their work, their system takes information from UIDAI in the electronic system. They designed four main stages of the system: Registration, Electorate information pages, Electorate voting phase, and Completion phase (Yadav, 2014)- (Vidyasree, P and Raju, S Viswanadha and Madhavi, G, 2016).

In 2017, Alexander Schneider presented a study on Remote Electronic Voting. In this survey, they discussed the schemas, attacks, and systems of remote electronic voting. According to this survey, the system should be available, integrated, and perform all the functions correctly such as counting, eligibility of voters, fairness, voter-verifiable, robustness, and Receipt freeness to reduce coercion. There are a lot of attack vendors and these attacks should be considered during the design of an electronic voting system (Sridharan, 2013). The electronic voting machine will increase voter participation. Elections will be fair by using Electronic Voting Machine. It refuses the frauds. If a vote has been correctly cast by the voter, he/she will receive confirmation. Votes can be count precisely and quickly and these systems can be implemented in large-scale elections such as presidential elections (Schneider, 2017). In 2016, a study about the Secure Online Voting System is presented. They discussed the different online voting systems based on homomorphic encryption, blind signature. The user does the registration process first. All the information has been sent to the authentication server. The server sends login to the voter. If this login is authenticated then the user is allowed to cast the vote and this system provides a secure casting system (Khairnar, 2016).

In 2017, a study on Biometrically Secured Electronic Voting Machine is presented in which the study on a fingerprint-based voting system is done. Each user vote has been verified using a fingerprint. Moreover, the user can also change the vote, if the vote is given to the wrong candidate. The controller unit of the whole system was Arduino. All the working of the voting system was displayed on LCD (Rezwan, 2017). In 2017, M.A Hosany presented a study on the Design and implementation of an online voting system for the election of students of the University of Mauritius. They designed a system that acted as client/server architecture. Their system comprised a web application, mobile client application, server application, and central database (Hosany, 2017)- (Hazzaa, 2012).

In 2018, a study on Blockchain-enabled E-voting is presented in which the BEV provide each voter a “wallet” that contain user credential. Employees of BEV have an encrypted key and also have temper

proof personal IDs, e.g. Mobile E-voting platform based on Boston startup have real-time ID and smart biometric. Hackers can be attacked on blocks before introducing new blocks, blocks are files with transaction records. Blockchain ensures that no block can be removed or changed. Temper-proof audit trails can be created by enabling Blockchains. It generates cryptography to keep records secure (Kshetri, 2018)- (Peck, 2015). The limitations of wired electronic voting are resolved by using a radio frequency identification (RFID) based electronic voting machine (EVM) with a fingerprint module. The voters will be authenticated using the fingerprint module. All voter information, including fingerprints, will be maintained in the database. The database is stored on the microcontroller. During polling, the microcontroller validates the voter by checking the database (Malathy, 2020).

A hacking system is presented in this research work is a simple GUI application that is based on JAVA and the whole software contains about 2000 lines of code. The GUI interface provides the user with easy to use and friendly interface for the voting process as this machine record the votes. After authentication of the user with the 4-digit pin, the machine allows the voter to cast a vote (Bannet, 2004)- (Kaliyamurthie, 2013). In this century, the fingerprint is a very useful method to recognize humans; automated biometric systems are used in recent years, with the help of it, work implemented and evaluated successfully. Results were comparable and significant. This proved that the recognition using fingerprint will be enhanced and improved the verification procedure because fingerprint has acceptance with the law enforcement, the forensic science community, and the general public, they will be utilized new systems that will require a biometric system in it. With the help of biometric procedures, there are high chances for fair elections (Mahajan, 2018)- (Nithya, 2016).

The paper-Based Voting system was a traditional way of voting but due to its unreliability and inefficiency, a new way of voting was introduced known as Electronic Voting and Internet Voting. It will increase voter participation. Elections will be fair by using Electronic Voting Machine (EVM) as it refuses the frauds. If a vote has been correctly cast by the voter, he/she will receive confirmation and votes can be count precisely and quickly. The proposed objectives of this research work are

- Using a Local/Centralized server.
- Encrypting traffic to/from a centralized server.
- Making the voting system more secure, reliable, faster, cost & time efficient.
- Maintain security using cryptography.
- Printing Form-45 on completion of the election.
- Development of software for Voting.

The electronic voting system is more efficient than our traditional style to cast votes (Adekunle, 2020). An electronic Voting Machine ensures flawless voting. This user-friendly electronic voting machine will be cost-efficient as well as time-efficient too.

The overview of the proposed EVM in Fig. 1 consists of four blocks. Fingerprint Scanner will scan the voter’s finger and pass the result to the software. The software will verify the user’s identity using this

fingerprint. QR code scanner will scan the voter's national identity card commonly known as CNIC. The QR code scanner will share a 25-digit string with the software. The software will parse this string and after parsing store the 13-digit string. This 13-digit string will be compared with the database to get the identity of the user. The Centralized Server will have complete data of voters. All the voting data will also be stored on a centralized server and the server traffic will be encrypted using SSL. The Local System will contain other parts like a fingerprint scanner and QR code scanner that will communicate with a centralized database and our frontend application will be running at Local System.

2. Materials And Methods

An Electronic voting machine that will be user-friendly and will prevent time loss is employed in which the software is divided into two parts under the law of the Election Commission of Pakistan. The two modules are

Authentication Module.

Voting Module.

On the voting day, the administrator will log in to the software and will set the voting duration and server. Following that, the administrator will begin the voting process. To confirm a voter's identity, the voter will scan his/her identity card, and if his/her name is found on the voting list, he will verify his/her fingerprints. After confirming his/her identity, he/she will proceed to the second machine where the voter will cast his/her vote. After the voting time has started, the voter will proceed to the first machine which is the authentication module (Walake, 20115). Here, the voter will scan his/her identity card, the machine will search his name in the database. If the name is found the machine will check if the voter has already voted or not. If the voter has not voted the machine will allow the voter to scan his/her fingerprint.

The voter will be able to select his/her desire finger to confirm his/her identity. If the voter has successfully verified himself/herself then the voter will proceed towards the voting module. In the proposed system, the voter will be able to select the candidate of his/her choice. After selecting the candidate, the machine will print the image of the selected candidate. The voter will put the image into the ballot box. The use of printed images and electronic votes will prevent fraud and rigging in elections and this will also be helpful in the recounting process.

2.1. System Architecture

This system architecture consists of both Software system and Hardware system.

2.1.1. Authentication Module

After logging in, the administrator can choose the time for voting as well as the server. The system will save the administrator's login time and date, as well as the total voting time set by the administrator. The

system will also record the start time of the voting. The authentication module will verify the identity of the voter using his CNIC number that the voter will verify using a QR Code Scanner. Moreover, a voter will also have the option to input his/her identity card number if he/she fails to scan the ID card in any case.

The system will decide if the voter has already voted or not after scanning the ID card; if the voter has already voted, the system will not enable the voter to vote again and will generate an error. If a voter is authorized to vote, he or she must use fingerprint verification to verify their identification. The System will allow the user to scan any finger/thumb. A screen will appear asking the voter, which finger/thumb he/she wants to scan to verify his identity. After selecting the required option, the user will be allowed to scan his/her fingerprint. Once the voter is verified, he/she will be allowed to vote.

2.2. Voting Module

The voting module consists of an Admin login too. After logging in, the admin can select the time of voting. The system will store the admin login time and date and will also store the total voting time set by the admin. The system will also store the time when the voting will begin.

The voting module will show the candidate list after the successful login of the admin and set the time. Once a voter is clear to cast his/her vote after passing through the authentication process then he/she will come to the booth where the voting module is present with the candidate list. The voter will select the candidate's mark. Once the mark is selected then the vote will be updated in the database and the same vote will be printed through the printer so that the voter can testify his vote and then cast this printed vote to the nearby ballot box this printed vote will be used for recounting which increase the accuracy and make voting more convenient.

After the voter casts his vote by selecting the desired candidates, the screen will not accept clicks for a short period to prevent multiple votes from a single user. The screen will then be disabled for a couple of seconds so that the voter can take his paper ballot and cast it in the ballot box. After that, the screen will start working again, enabling the next voter to cast his or her vote. After each vote is cast, the system will check for the remaining time. Once the time is up, the system will go to a screen that requests an id and password. The administrator will enter his id and password into that form. After verifying the id and password, the next screen will provide the results that can be printed in the same way as form 45 does.

2.3. Design Specifications

Design specifications include specifications of hardware and software discussed under 'System architecture'.

2.3.1. Screen

It is the main part/ hardware of this system. It is a platform where the user has to cast the vote using the touch screen. Different hardware for authentication and printing procedure will be attached with a

computer system including fingerprint device, QR code scanner, and printer. Following are the detail and specifications of all these hardware devices.

Table 1
Specification of Hardware
screen

Manufacture	**1080 * 1920**
Frequency	60Hz
Screen Size	13” diagonal
Touch	Yes

For authentication, this system will use a fingerprint device and QR code scanner. Following are the detailed specification of the fingerprint device and QR code scanner.

2.3.2. Finger Print Scanner

In the authentication module, Fingerprint Reader is used to verify the voter’s identity. The fingerprint reader scans the voter’s fingerprint and extracts the minutiae. Then it compares the fingerprint with the enrolled fingerprint of a voter. The Digital Persona URU 5100 Fingerprint Reader is used for fingerprint reader devices.

The specifications of fingerprint scanning device can be depicted in Table 2.

Table 2
Specifications of fingerprint device

Manufacture	**Digital Persona Inc.**
Connection	USB 2.0
Supported OS	Microsoft Windows, Linux & Android
Resolution	500ppi
Image Capture Area (Platen Size)	13 * 17 (0.5” x 0.6”)
Sensor type	Optical
Illumination	Blue LEDs
Operating Temperature	0° ~ + 40°C
Operating humidity	20–80 % (non-condensing)
Device Size	72 * 39 * 22 mm (2.8” * 1.5” * 0.9”)
Device weight	84 rams (3.0 oz)

2.3.3. QR code/ Barcode scanner

This bar code reader is a plug-and-play. Honeywell 2D Barcode scanner is used for the execution of EVM. The specifications of the Honeywell 2D Barcode scanner are given in Table 3.

Table 3
Specifications of QR code scanner

Light Source	**White LED**
Sighting Device	Red LED, 617nm
Interface	USB
Scanning Type	Image
Decoding Capability	All standard 1D and 2D Bar Codes
Weight	146g
Input Voltage	4 ~ 5.5 V DC
Bar Code Density	Depth of field
Resolution	4 mil
Tolerance	100mm/sec 13 mil UPC

2.3.4. Printer

When the vote has been cast successfully, it should be printed using the laptop interface. After Casting a Vote on an electronic voting machine, the voter has to put his/her printout of the vote into the ballot box. The specifications of the Xprinter used in the proposed model can be observed in Table 4.

Table 4
Specifications of Printer

Manufacture	**Xprinter**
Connection	USB 2.0
Supported OS	Microsoft Windows, Linux
Print Size	79-80mm
Column Capacity	576 dots/line or 512 dots/line
Command	Compatible with ESC/POS
Operating Temperature	0° ~ + 45°C
Operating humidity	10 – 80 %

2.4. Specifications of Software

A software is developed to confirm the identity of the voter. The software allows the administrator to log in and set the time and server for the voting. When the administrator logs into the software, the software saves the login time against the administrator's unique id. This one-of-a-kind id is the primary key that will be used to identify the administrator. The overall voting time and the voting ending time set by the administrator will also be saved in the database by this software. After selecting the server, the administrator will begin the voting. The voter will have the option to scan his/her identity card or input the number of his identity card if he/she fails to scan the identity card in any case.

The software will check if the voter has voted before after scanning the identity card. If not, the system will allow the user to scan his/her desired finger to verify his identity. If the voter successfully confirms his/her identification by fingerprint scanning, he/she will be directed to the voting module to cast their vote. If the voter has failed to confirm his/her identity against the provided identity card number, then he/she will not be allowed to proceed towards the voting module. NetBeans 8.2 software is used to develop the Program for authentication of the voter. To store the information and fingerprints of the voter, MYSQL server 8.0 on Red Hat Enterprise Linux 7.5 software is used.

3. Implementation Of Electronic Voting Machine

Following the design of the EVM, the software and hardware structure must be implemented. As a result, the EVM implementation is further divided into two parts. The first section describes the server's implementation and configuration for remote access. The second section describes the software implementation, which is further divided into two parts.

3.1. Implementation of Authentication Module

A software is developed to confirm the identity of the voter. The software allows the administrator to login into the software and set the time and select the server for the voting. As soon as the admin logins into the software, the software will save the login time against the admin’s unique id. This unique id is the primary key that will be used to identify the admin. This software will also save the total voting time and voting ending time set by the admin.

After selecting the server, the admin will begin the voting. After voting is started by the administrator, the voter will have the option to scan his/her identity card or input the number of his identity card, if he/she fails to scan the identity card in any case. After scanning the identity card, the software will check if the voter has voted before or not. If not, the machine will allow the user to scan his/her desired finger to confirm his identity. If the voter is successfully in confirming his/her identity using fingerprint scanning, then he/she will be allowed to proceed to the voting module to cast the vote. If the voter has failed to confirm his/her identity against the provided identity card number, then he/she will not be allowed to proceed towards the voting module.

Before starting the authentication module, the admin needs to login into the software. To log in, the admin requires a username, password, and unique ID. The unique ID will be used to identify the admin

login status, starting time of voting, and the total timer set by the admin for voting. The username, password, and unique ID will be provided to the admin by the Election Commission of Pakistan.

After successful login into the software, the settings menu will appear before the admin. Using this settings menu, the admin will be able to select the type of server and the time of voting. The admin can select local, centralized, or both options from server settings. If the centralized server is selected, then before sending a query to the server the software will check either internet is available or not. If due to any reason the internet is unavailable, the software will automatically contact the local server. This process will happen every time the software needs to communicate with the centralized server.

In this window, the admin will set the voting time. This voting time will also be saved in the database against the id of the admin. Once the voting time is expired, the software will automatically log off.

Once this window appears, the voting process will start. The voter will have the option to scan his/her National Identity Card or enter the number.

If the voter fails to scan his/her ID card in any case, he/she can enter the number of ID card. Once the voter enters his/her ID card then the system will contact the server to check if the voter exists or not. If the voter exists and he has not voted before then the next screen will appear where the voter can select his desired finger to scan to verify his identity.

In this screen, the voter will be asked to select the finger he/she wants to scan to confirm his/her identity against the provided CNIC number. The machine will have all the voter's fingerprints and the voter has the total choice to select the finger he/she wants to scan.

Now the voter can scan his/her fingerprint using the fingerprint reader. If the voter has verified himself/herself against the entered identity card number, then he/she will be allowed to vote and the database will be updated and a Boolean value will be set to true which means the voter won't be allowed to vote again.

3.2. Centralized Server Working

In this machine, a centralized server is connected that contains the data of all voters. To explain the working of the centralized server a physical example is considered. The voter is not registered in the current area or he/she belongs to some other city and the voter wants to cast his vote in this area. The voter will scan his/her identity card number. After scanning, the machine will check either the voter is registered in the current area or not. If the voter is not registered in the current area, the machine will automatically send a request to a centralized server to check where the voter is registered. After determining the location of the voter the machine will also check if the voter has already voted or not.

After confirming the identity, the machine will print a QR code for the voter. The voter will collect the printed QR code slip and will proceed to the next machine which is the voting machine. Here the user will scan his/her slip and the candidates of his registered area will be shown to the voter. The voter will select

his/her desired candidate and the machine will print the selected candidate on a page. The voter will collect the slip and will deposit it in the ballot box. To prevent voting again from the same QR code slip the machine will store the National Identity Card number of the voter on the local server. If the same QR code slip is scanned again, the machine will not display any candidates and this will prevent the voter to cast the vote again.

3.3. Implementation of Voting Module

The developed software is used to cast the vote. This software allows the admin to login into the software and set the time and select the server for the voting. As soon as the admin logins into the software, the software will save the login time against the admin's id. This software will also save the total voting time and voting ending time set by the admin. The working of the proposed software is based on requirement engineering that is used to describe that what a software system should do to satisfy the formal and informal requirements of the system.

The voting will begin after the admin has set the specific time. The voter list will be displayed on the screen, allowing the voter to choose the candidate of their choice. Following the selection of a candidate, the vote will be automatically updated in a database and printed on a printer before being cast into the ballot box. When the voting time will end, the admin will be able to print Form-45.

Before Starting the voting module, the admin needs to login into the software. To log in, the admin requires a username and password. The username will be used to identify the admin login status, starting time of voting, and the total timer set by the admin for voting. The username and password will be provided to the admin by the Election Commission of Pakistan.

After successful login into the software, the settings menu will appear before the admin. Using this settings menu, the admin will be able to set the time of voting.

In this window, the admin will set the voting time. This voting time will also be saved in the database against the id of the admin. Once the voting time is expired, the software will automatically log off.

After setting the time, the window will appear for confirmation of voting to start voting. When the voting process will start, the window will appear containing ballot paper. Each sign is clickable, one of them will be selected by the voter to cast the vote.

Once the voter will select any of the signs of his/her desire candidate, the voting database will be updated and the vote will be printed and the screen will be disabled for a while till the next voter will come to cast the vote. This screen does not contain any other control options like close or minimize to avoid any unconvinced. After the voting time will end, this screen will automatically disappear and the admin will be able to print Form-45.

4. Results And Discussion

4.1. Unit Testing

Testing provides an ease to troubleshoot or identify design and implementation flaws. Therefore as soon as the development stage was completed, the developed module was tested against relevant requirements. In most phases, the system was tested overall. However, unit testing was done after the complete implementation described in the previous chapter. Following are the testing of different units used in Electronic Voting Machine.

4.1.1. Testing of Fingerprint Module

In the authentication module, we have used Digital Persona URU 5100 Fingerprint Reader to verify the voter's identity. The accuracy of the fingerprint reader is 100% because the fingerprint reader supports counterfeit finger rejection. Another aspect that improves security is that the device scans fingerprints from four distinct angles when enrolling the fingerprint. CNIC is used to get the fingerprint of the vote against it. Then the stored fingerprint is compared with the fingerprint that is scanned using the fingerprint device. This will reduce the percentage of the error to a bare minimum

4.1.2. Testing of Printer

In the Voting module, Xprinter is used to print the casted vote. The accuracy of the Xprinter is 100% as it works on programming commands. That's why the percentage of error is reduced to a minimal. Table 5 depicts an evaluation of equipment based on the novel method of requirement engineering.

Table 5
Unit Testing

ID	Priority	Name	Status	Remarks
UT-01-001	1	Fingerprint device	**OK**	Achieved
UT-01-002	2	QR code scanner	**OK**	Achieved
UT-02-003	1	Printer	**OK**	Achieved

4.2. Functional Testing

After the successful unit testing, functional testing was done. In most phases, the system was tested overall. However proper functional testing was done after complete implementation described in Sect. 3. It includes the Functional requirements, containing quality attributes of the system whereas non-functional requirements, that constitute Software Requirements Specifications (SRS). SRS is the description of that what software will do.

4.2.1. Functional Requirement Testing

The technical requirement of the system is Functional requirements. It tells us that what our system will do. Functional requirements evaluation of the implemented system is described in Table 6.

Table 6
Functional requirements Evaluation

ID	Priority	Description	Status	Remarks
FR-01-001	1	Using Local server	**OK**	Achieved
FR-01-002	1	Using centralized server	**OK**	Achieved
FR-01-003	1	Implementing SSL	**OK**	Achieved via programming
FR-02-001	2	Printing Form-45	**OK**	Achieved
FR-02-002	2	Encryption	**OK**	Achieved

4.2.2. Non-Functional Requirements Evaluation

Requirements that are used to judge the operation of the system in particular condition are Non-functional requirements. It describes that how the system will perform different functions. So, the Non-Functional requirements evaluation of this system is discussed in Table 7.

Table 7
Non-Functional Requirements Evaluation

ID	Priority	Description	Status	Remarks
NFR-02-001	2	Reliability	**OK**	This system is reliable because the votes are counted automatically
NFR-02-002	2	Security	**OK**	The system is secure due to the implementation of SSL.
NFR-02-003	2	Efficiency	**OK**	The efficiency of EVM is 100%
NFR-02-004	2	Reusability	**OK**	After the election procedure, this machine will be used in the next elections
NFR-02-005	2	Faster	**OK**	Fast and reliable system due to its automatic functioning
NFR-02-006	2	Integrity	**OK**	This system is designed to keep the secrecy of the votes using encryption
NFR-03-001	2	Standard	**OK**	Meet all the electronic voting standards that ensure the security to overcome the bogus votes
NFR-03-003	2	Legislative	**OK**	This product is own design and does not have any legislative issue of copyright etc.
NFR-03-004	2	Environment friendly	**OK**	Our system is user friendly due to its user-friendly environment
NFR-03-005	2	Cost	**OK**	Optimal Cost
NFR-03-006	2	Time	**OK**	Deadlines followed.
NFR-03-007	2	Throughput	**OK**	Satisfactory throughput achieved

After thorough testing, we proceeded towards the investigation of our implemented techniques and verified whether desired functionality has been achieved. This system contains two parts Authentication module and the voting module. Following are the results of both modules

4.3. Results of the authentication module

When a fingerprint is added into the fingerprint device it works accurately because it scans the finger according to the QR code scanner. Moreover, proposed systems also differs from existing systems as it contains the options to adding any fingerprint. This option will increase voters to cast their votes according to their ease.

This system is secure because it ensures that one person can cast vote only once. And its communication is secured with SSL (Secure Socket Layer). Every vote is encrypted so there is the least chance for unfairness in Elections. The proposed system ensures data security as no one can change or modify the information of the voter. Even the administration cannot change or modify the records of a voter

The voter has to add his/her finger with various angles to ensure that the finger is enrolled successfully. This system is designed to keep the vote secret through encryption to and this way we ensure integrity. Communication of encrypted data between server and machine will be secured using SSL.

When fingerprint was added successfully, a window appeared to inform that fingerprint is according to the QR code scanner and voter-verified.

Through this fingerprint scanning, the voter verifies that his/her vote is cast or not, or once the vote has been cast it cannot be changed by any person after casting. It will be protected until it is counted. No one will be allowed to cast vote more than once.

4.3.1. Probability of Accuracy

People who work/live in the village also have to cast their vote. So, we have to add fingerprints of all people living in the village. While taking fingerprints of people of rural, it was noted only 34% population of the village have complete/accurate prints on their right finger. One of the possible reasons is that the fingerprints of some old people are faded especially of those who do labor work in the village. Almost 79% of people have accurate/complete fingerprints on two fingers.

4.3.2. Database

In the implemented system data of 500 people is added into the database for validation of results. So, the proposed system is a prototype model that allows 500 authenticate voters to cast their votes.

4.4. Results of Voting Module

The voting module is tested for its real-time verification by casting the votes, the track of administrator login, and its login status is kept save in the database. To verify the working of the proposed voting

module, the allotted time for the voting is checked and tracked against 100 users and the accurate results can be verified from Fig. 24.

After that, the voting process is tested by casting votes to see if a user could cast multiple votes at once by touching the screen. The list of selected voters can be observed in Fig. 25. By disabling the listeners, it was ensured that one voter could only cast one vote at a time, and by disabling the controls, it was ensured that the voter could not exit or minimize the screen without casting vote. Thus the voting process continued to work successfully that ensures the reliability of the proposed EVM.

The voting module is tested and verified through random voting. We have added data of some voters into the database and then allow them to cast their vote. The voter only has to use a touch screen and select only one of the signs from the ballot paper to cast his vote successfully that can be depicted in Fig. 26.

Then voter clicked or touched on the BAT sign, the selected item printed through the printer and can be seen in Fig. 27. The proposed EVM will increase voter participation thus the elections will be fair and it refuses the frauds. If a vote has been correctly cast by the voter, he/she will receive confirmation. Votes can be count precisely and quickly.

This system will count votes automatically so the counting process will much faster and accurate than our traditional style of voting. The proposed system is convenient and reliable as it will be easy to use. It can handle voter data confidentially as it will save the record in its database. The result will be faster and efficient as compared to a paper-based voting system and people elect their most acceptable leader to lead them by using their right to vote.

5. Conclusions

The paper-based voting system is not reliable for fair polls especially in under developing countries. The electronic voting machine proposed in this work would bring a revolutionary change in election procedures. The existing EVM contained several drawbacks and one of the major drawbacks was having both modules on the same machine. The proposed EVM has been designed to overcome the shortcomings of existing systems. It includes fingerprints, ID scanners, and printers through which the public can elect their right representative more smartly and securely. Moreover, it will ensure that votes are encrypted and the results are declared on time by using SSL to ensure the security of the system. Following two modules and a server.

- Authentication module
- Voting module
- Centralized Server

In the system, both machines are operated using a touch screen. The first machine was used as an authentication module with a touch screen, fingerprint reader, QR code scanner, and printer embedded

with it. The printer works in case the voter is not registered in the same area and is verified using a centralized server. In further, the printer prints a QR code containing the CNIC number and the area code of the registered location. A second machine is a voting machine that contains a touch screen embedded with a QR code scanner and printer. It can include automatic vote counting, fingerprint scanning, a more efficient registration process, the storage and processing of results, and the declaration of results. As a result, duplicate voting, incorrect registration, fake biometrics, and late results declaration can be avoided for corruption-free elections. The proposed system is also helping to increase voter participation and reduces electoral rigging. Through the proposed system, if a voter has correctly cast vote, he/she receives confirmation by receiving the casted vote through a printer. The votes are counted precisely and quickly that makes the system more accurate and reliable. Conclusively, we can claim that the proposed system is a more secure, reliable, time-efficient, and cost-effective software-based approach.

Declarations

Funding

No Funding Source.

Conflicts of Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship and/or publication of this article.

Author Contributions

Conceptualization, J.A., and F.A.; Methodology, F.A., A.K., and M.I.; Software, J.A., S.M., and A.K.; Validation, A.A., M.I, and F.A.; Formal Analysis J.A., F.A. and S.M.; Resources, J.A., and M.I.; Writing-original draft preparation, J.A. and A.K.; writing-review and editing, A.K., S.M. and F.A.; Supervision, F.A.; Funding acquisition, No. All authors have read and agreed to the published version of manuscript.

Data Availability

Manuscript have no Associated Data.

References

1. Adekunle, S. E. (2020). A Review of Electronic Voting Systems: Strategy for a Novel. *International Journal of Information Engineering & Electronic Business, 12*(1).
2. Bannet, J. a. (2004). Hack-a-vote: Security issues with electronic voting systems. *IEEE Security & Privacy, 2*(1), 32-37.
3. Hazzaa, F. I. (2012). Web-Based Voting System Using Fingerprin Design and Implementation. *International Journal of Computer Applications In Engineering Sciences ISSN*, 2231–4946.

4. Hosany, M. a. (2017). Design and implementation of an online voting system for the election of students of the University of Mauritius. *Int. J Adv. Res. Comp. Eng. Technol, 4*(7), 4321-4327.
5. Irani, B. (2018). A beginner's guide to Electronic Voting Machines. Dhaka Tribune.
6. Kaliyamurthie, K. a. (2013). Highly secured online voting system over network. *Indian Journal of Science and Technology, 6*(6), 4831-4836.
7. Khairnar, S. a. (2016). Survey on secure online voting system. *Int J Comput Application, 134*(13), 19-21.
8. Kshetri, N. a. (2018). Blockchain-Enabled E-Voting. *IEEE Software, 35*(4), 95-99.
9. Kumar, D. A. (2012). Electronic voting machine—A review. *IEEE* (pp. 41-48). IEEE.
10. Mahajan, M. a. (2018). *M-Vote (Online Voting System).*
11. Malathy, V. a. (2020). Radio frequency identification based electronic voting machine using fingerprint module. *Conference Series: Materials Science and Engineering, 981*(3), 032018.
12. Mithe, R. a. (2013). Optical character recognition. *International journal of recent technology and engineering (IJRTE), 2*(1), 72-75.
13. Nair, D. G. (2015). An Improved E-voting scheme using Secret Sharing based Secure Multi-party Computation. *arXiv preprint arXiv:1502.07469*.
14. Nithya, S. a. (2016). Advanced secure voting system with IoT. *International Journal of Engineering and Computer Science, 5*(3), 16033–16037.
15. Peck, M. (2015). The Future of the Web Looks a Lot Like the Bitcoin Blockchain. *Retrieved January, 7*, 2018.
16. Rezwan, R. a. (2017). Biometrically secured electronic voting machine. In *2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC)* (pp. 510-512). IEEE.
17. Schneider, A. a. (2017). Survey on Remote Electronic Voting. *arXiv preprint arXiv:1702.02798*.
18. Shahzad, B. a. (2019). Trustworthy electronic voting using adjusted blockchain technology. *IEEE Access, 7*, 24477–24488.
19. Sridharan, S. (2013). Implementation of authenticated and secure online voting system. *Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT).*
20. Srikrishnaswetha, K. a. (2019). A study on smart electronics voting machine using face recognition and Aadhar verification with IOT. In *Innovations in electronics and communication engineering* (pp. 87-95). Singapore: Springer.
21. Vidyasree, P and Raju, S Viswanadha and Madhavi, G. (2016). Desisting the Fraud in India's Voting Process through Multi Modalbiometrics. *IEEE 6th International Conference on Advanced Computing (IACC).*
22. Walake, M. A. (20115). Efficient voting system with (2, 2) secret sharing based authentication. *International Journal of Computer Science Information Technology, 6*(1), 410-412.
23. Yadav, V. K. (2014). An approach to Electronic Voting System using UIDAI. *International conference on electronics and communication systems (ICECS).*

24. Yang, X. a. (2018). A secure verifiable ranked choice online voting system based on homomorphic encryption. *IEEE Access, 6*, 20506–20519.
25. Yi, X. a. (2013). Practical Internet voting system. *Journal of Network and Computer Applications, 36*(1), 378-387.

Figures

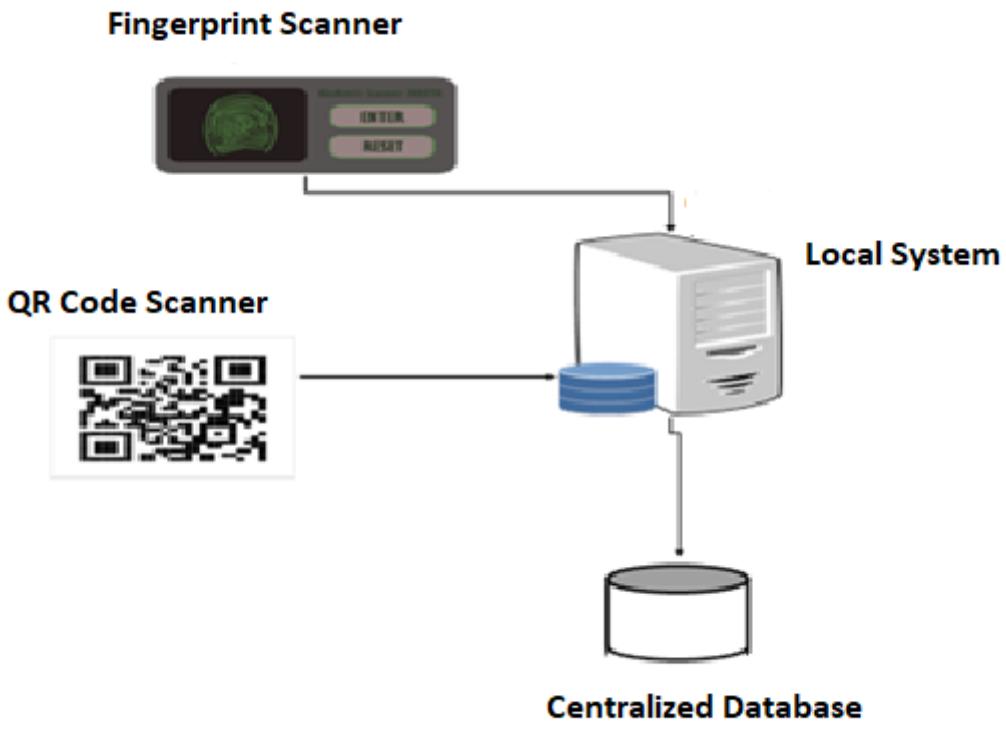

Figure 1

Overview of the Proposed Electronic Voting Machine

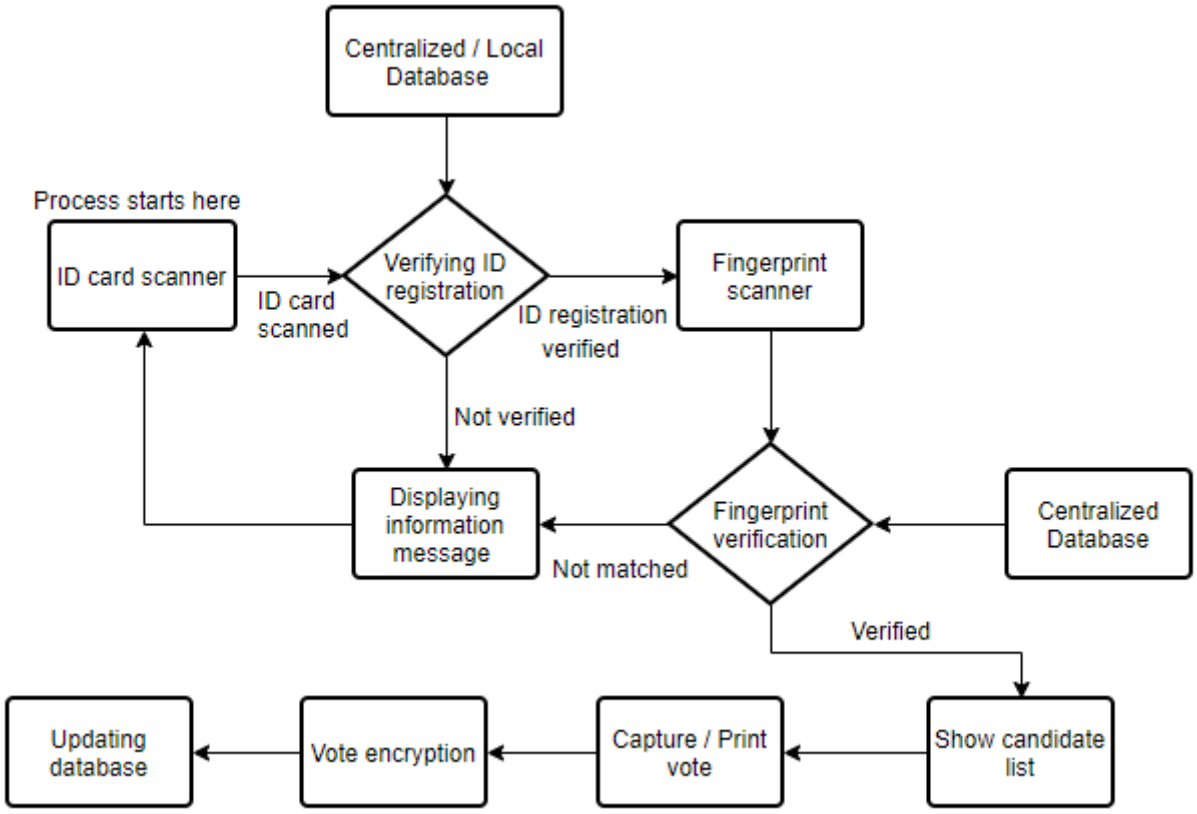

Figure 2

Methodology of Working Model

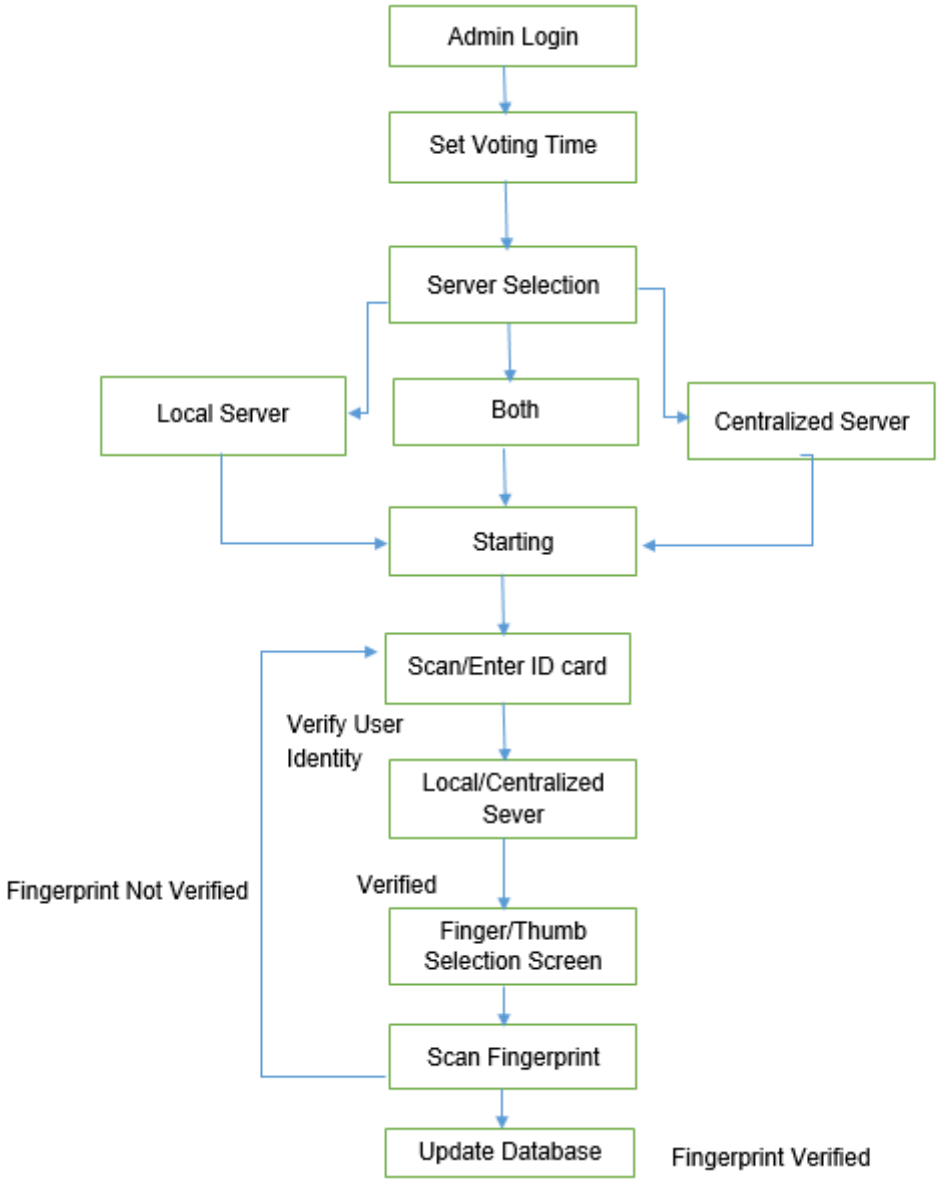

Figure 3

Flow Chart Model of Authentication Mode

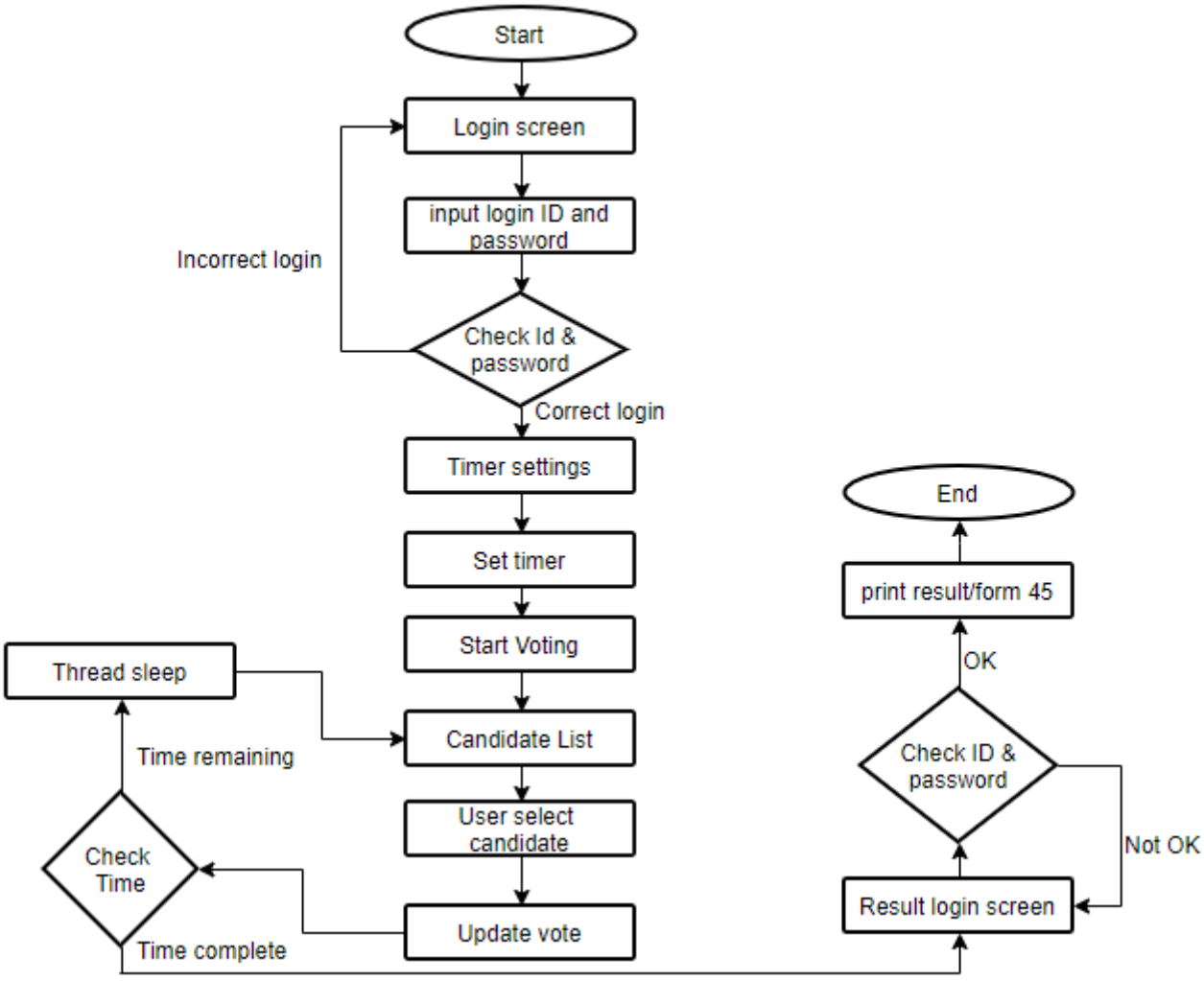

Figure 4

Flow Chart Model of Voting Module

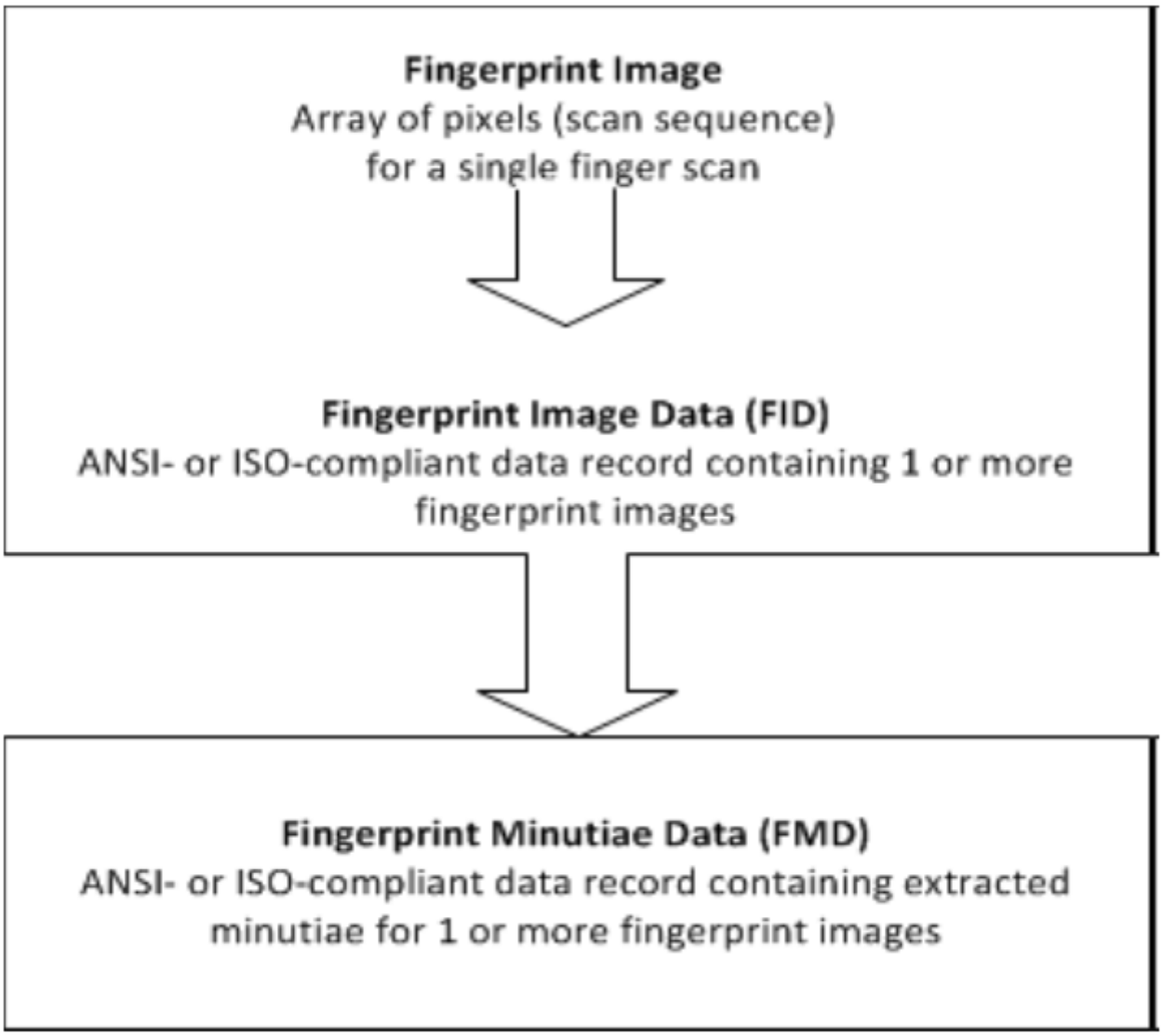

Figure 5

Dataflow used by U are U SDK

Figure 6

Login screen preview

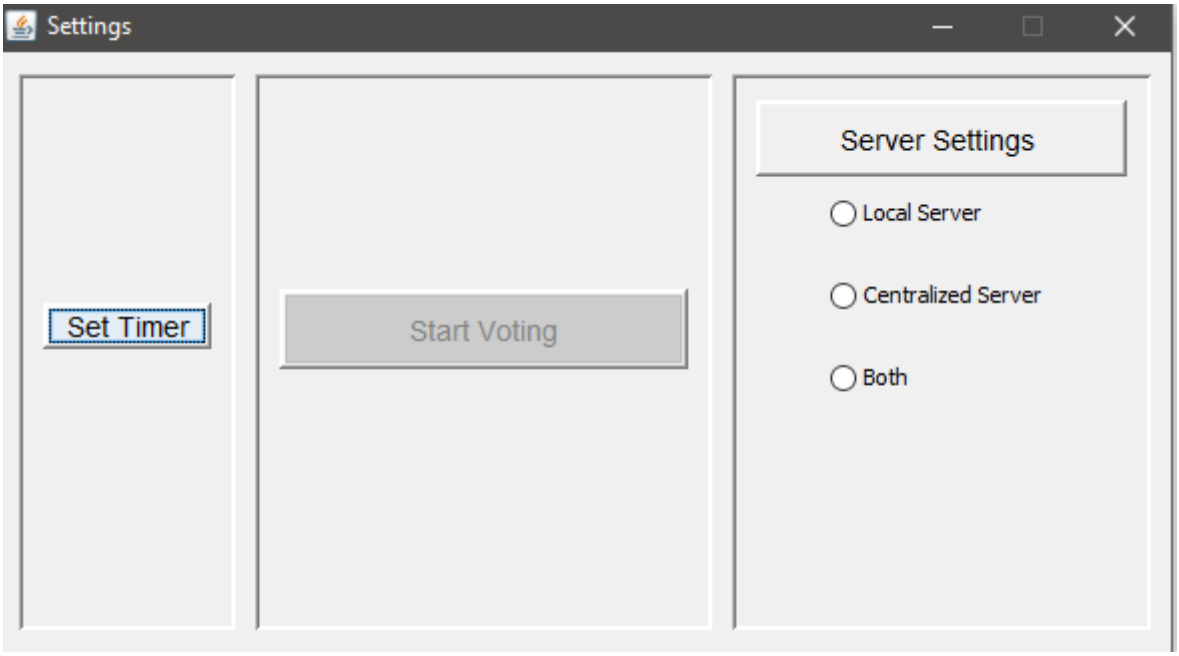

Figure 7

Setting Mode

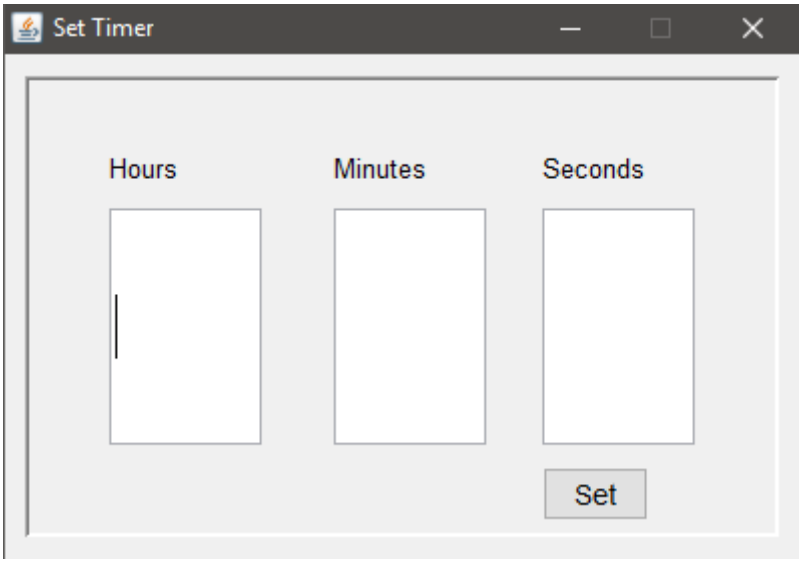

Figure 8

Timer setting window

Figure 9

ID card scanning window

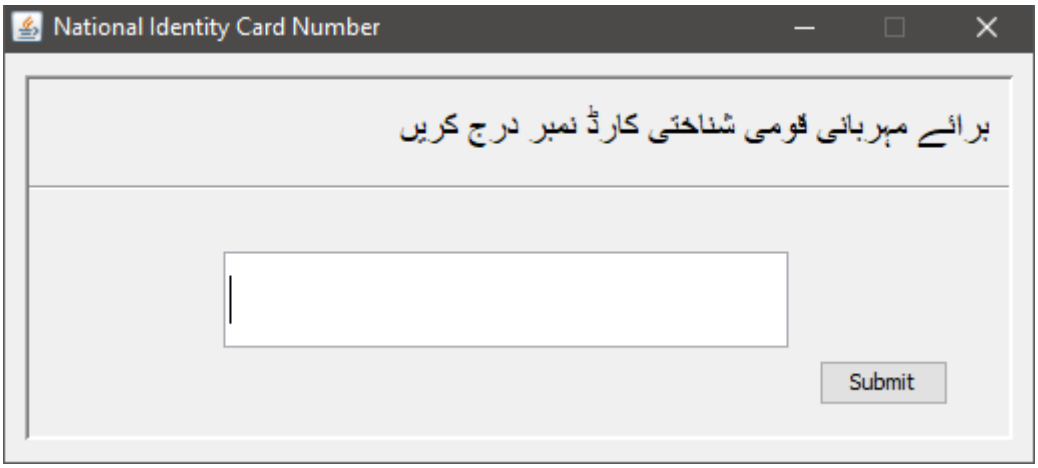

Figure 10

Enter ID card

Figure 11

Fingerprint selection screen

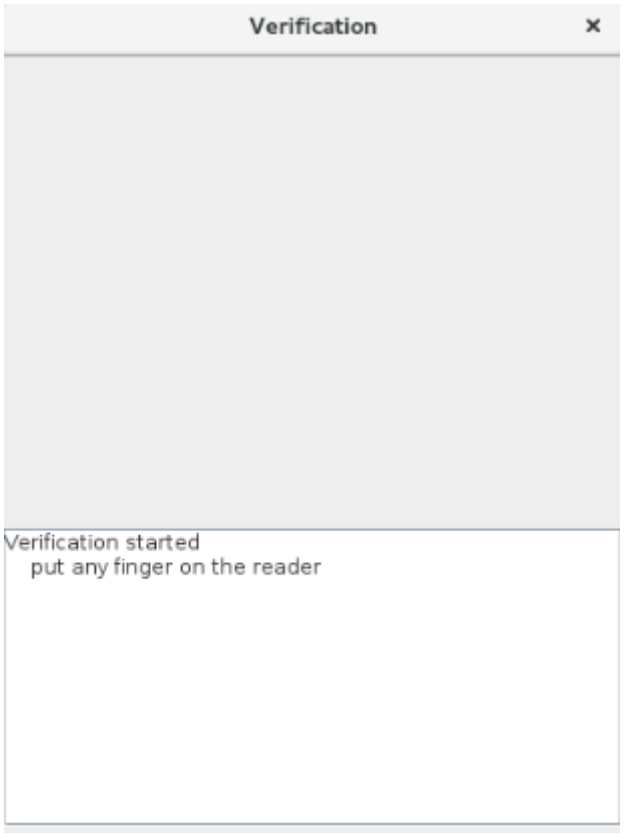

Figure 12

Verification screen

Figure 13

Login screen

Figure 14

Setting Mode

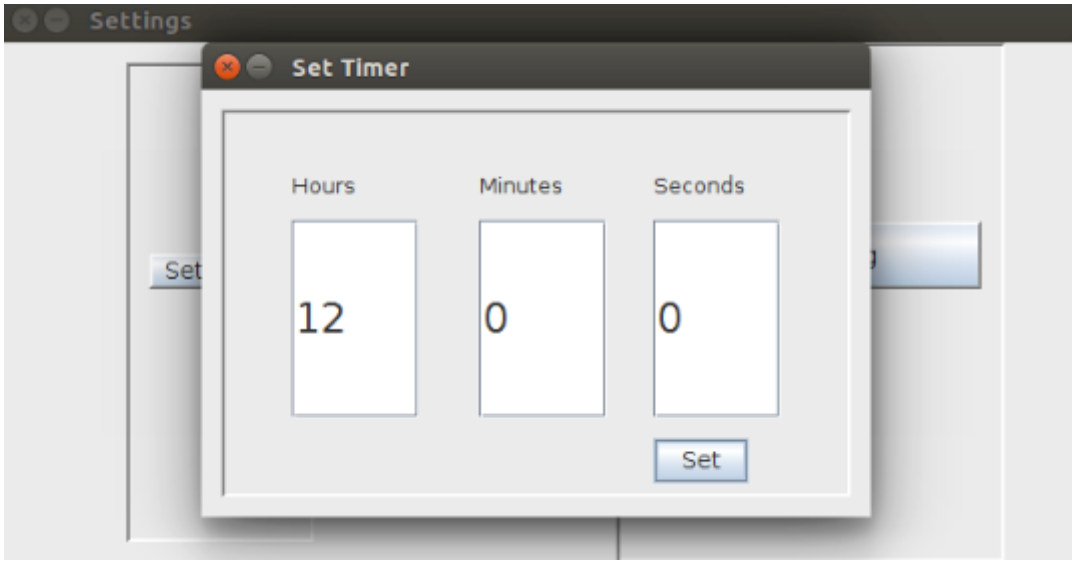

Figure 15

Set timer

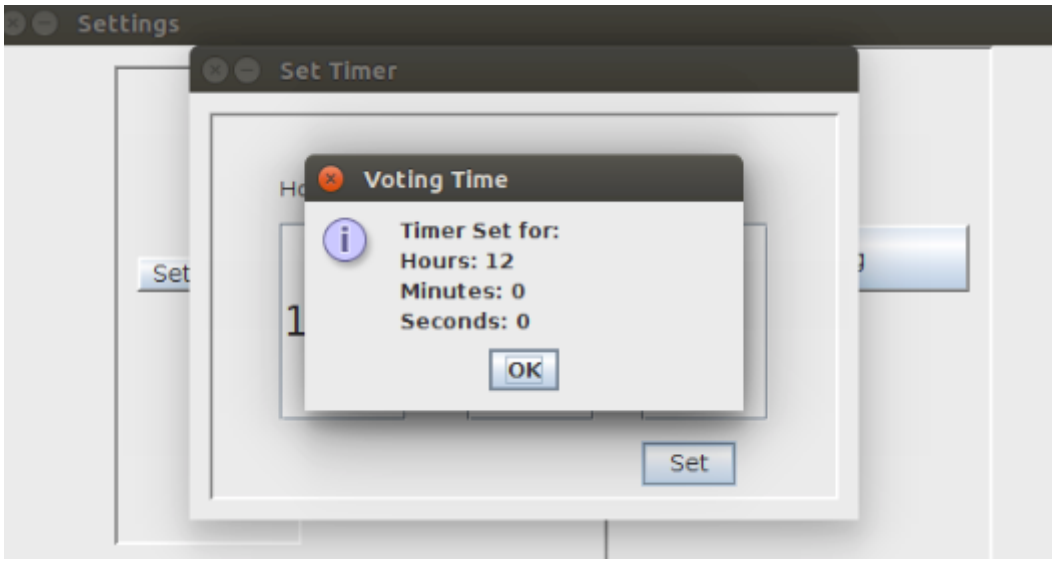

Figure 16

Set voting time

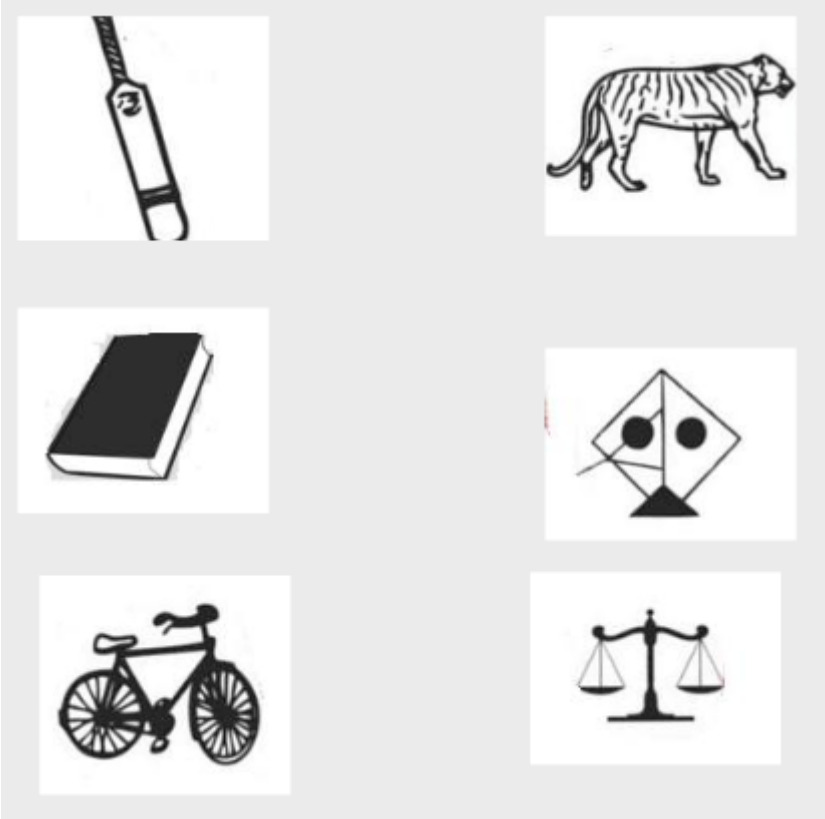

Figure 17

Ballot paper

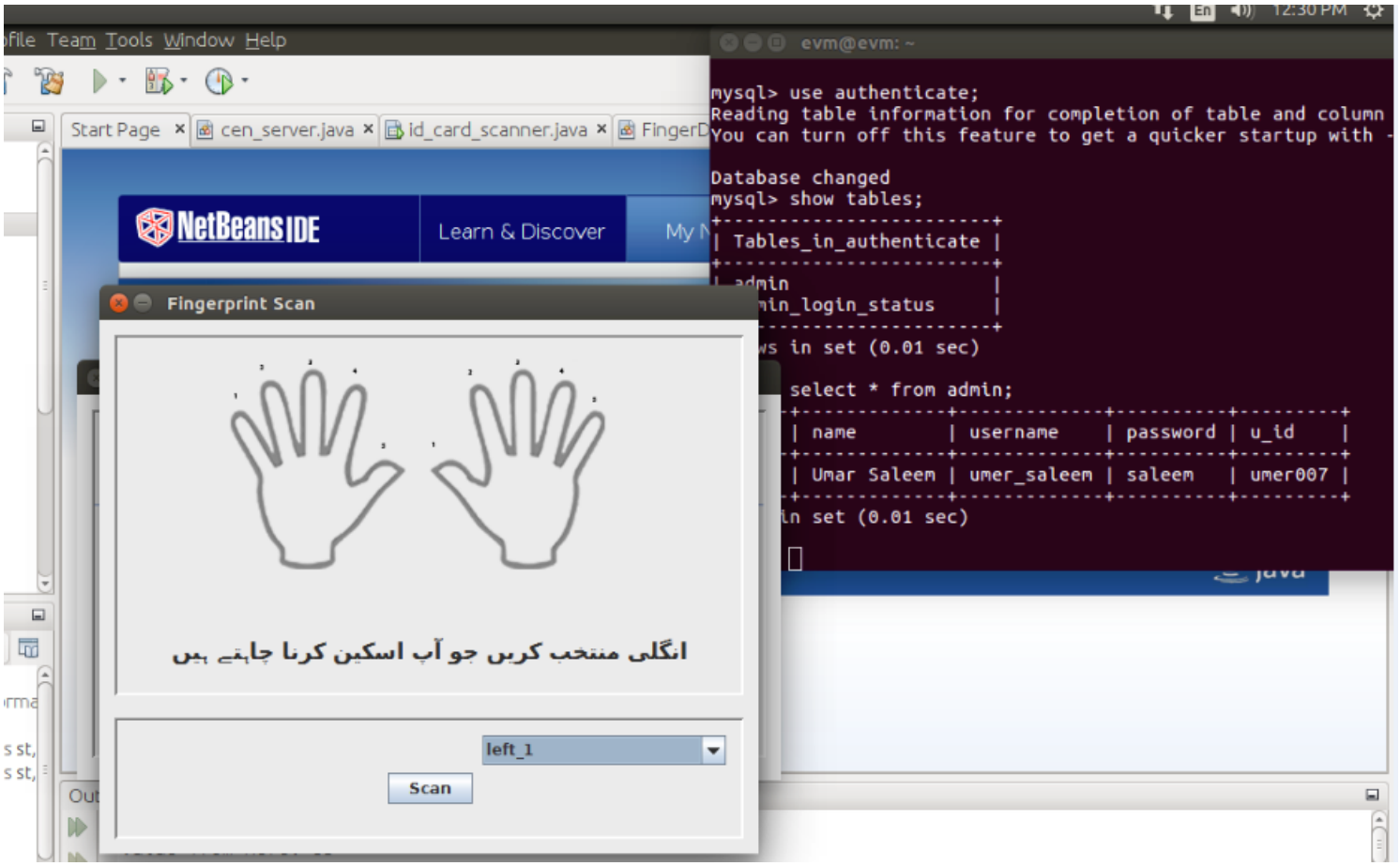

Figure 18

Select any window preview

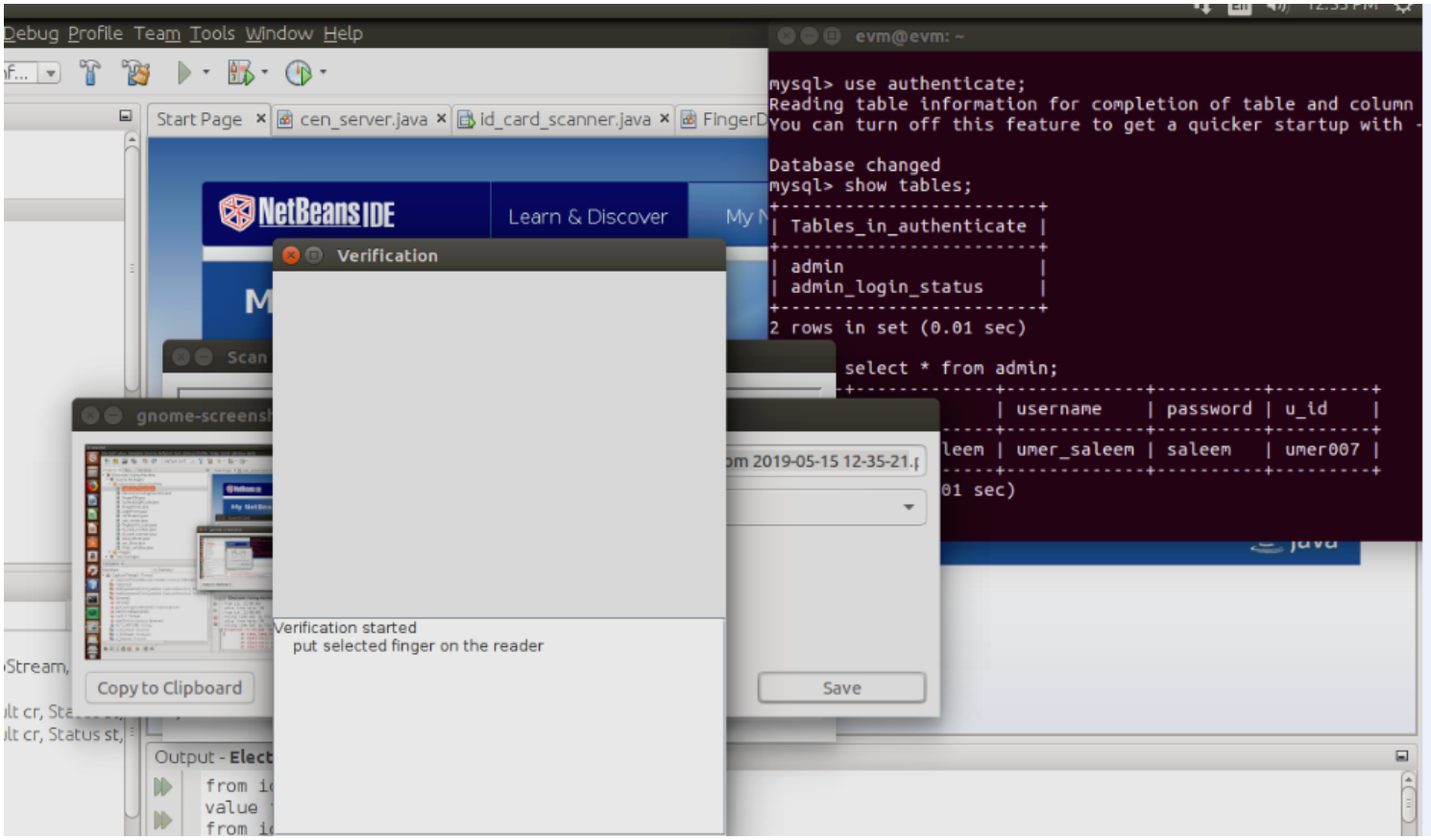

Figure 19

Fingerprint preview

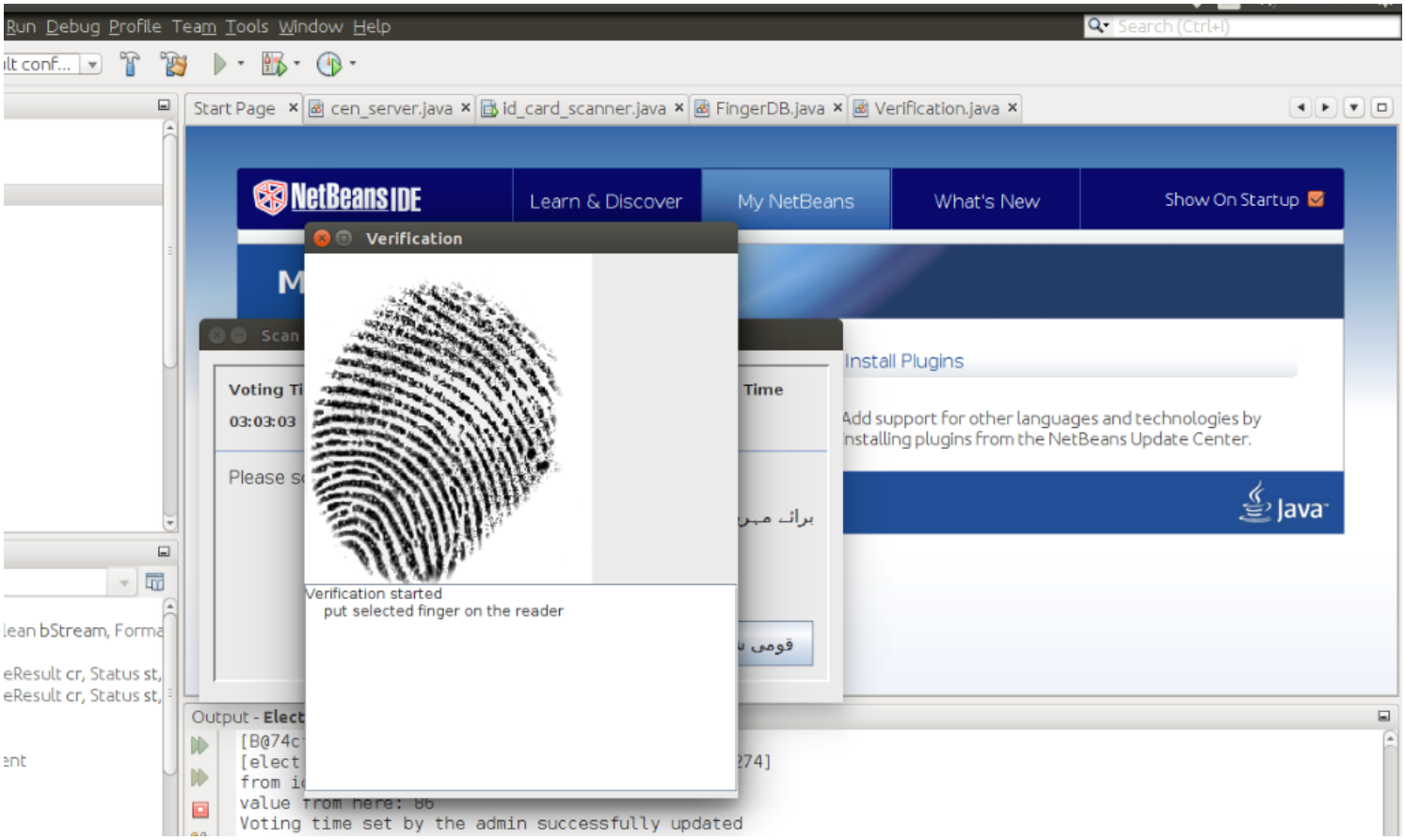

Figure 20

Fingerprint preview with different angles

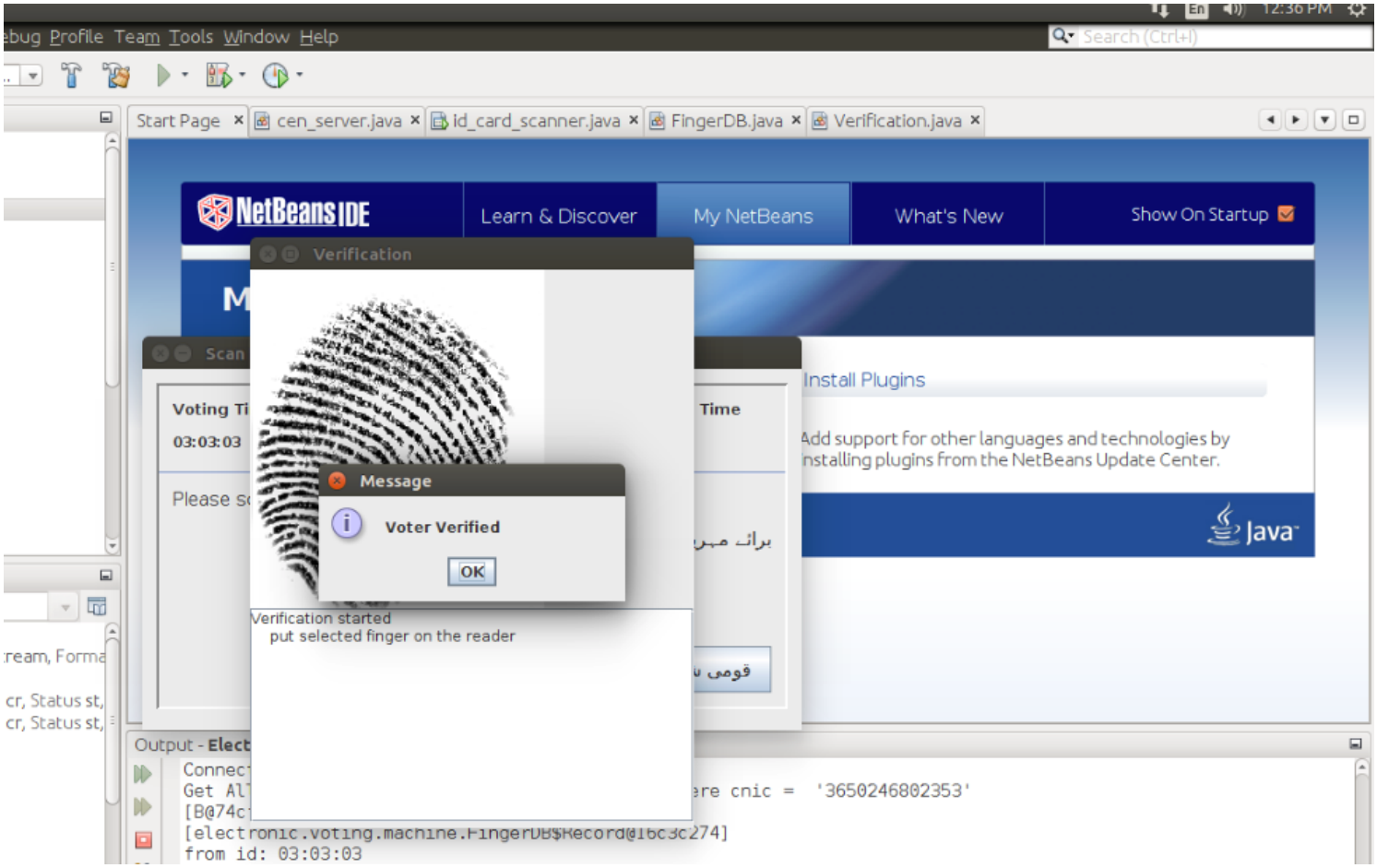

Figure 21

Voter verified window

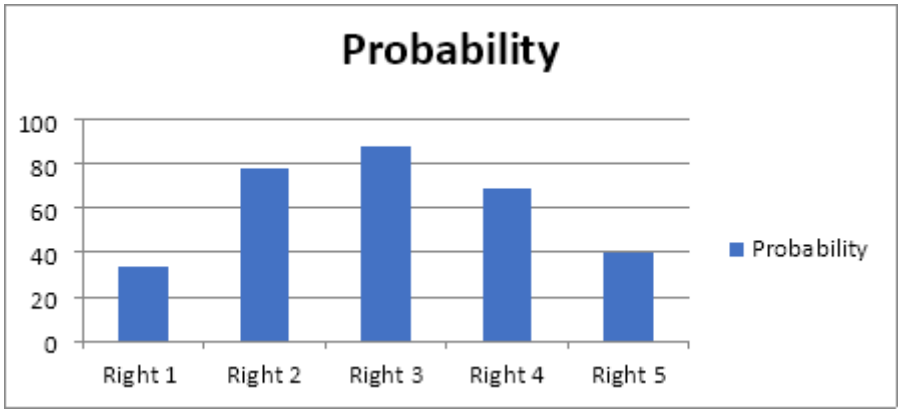

Figure 22

Probability of accuracy

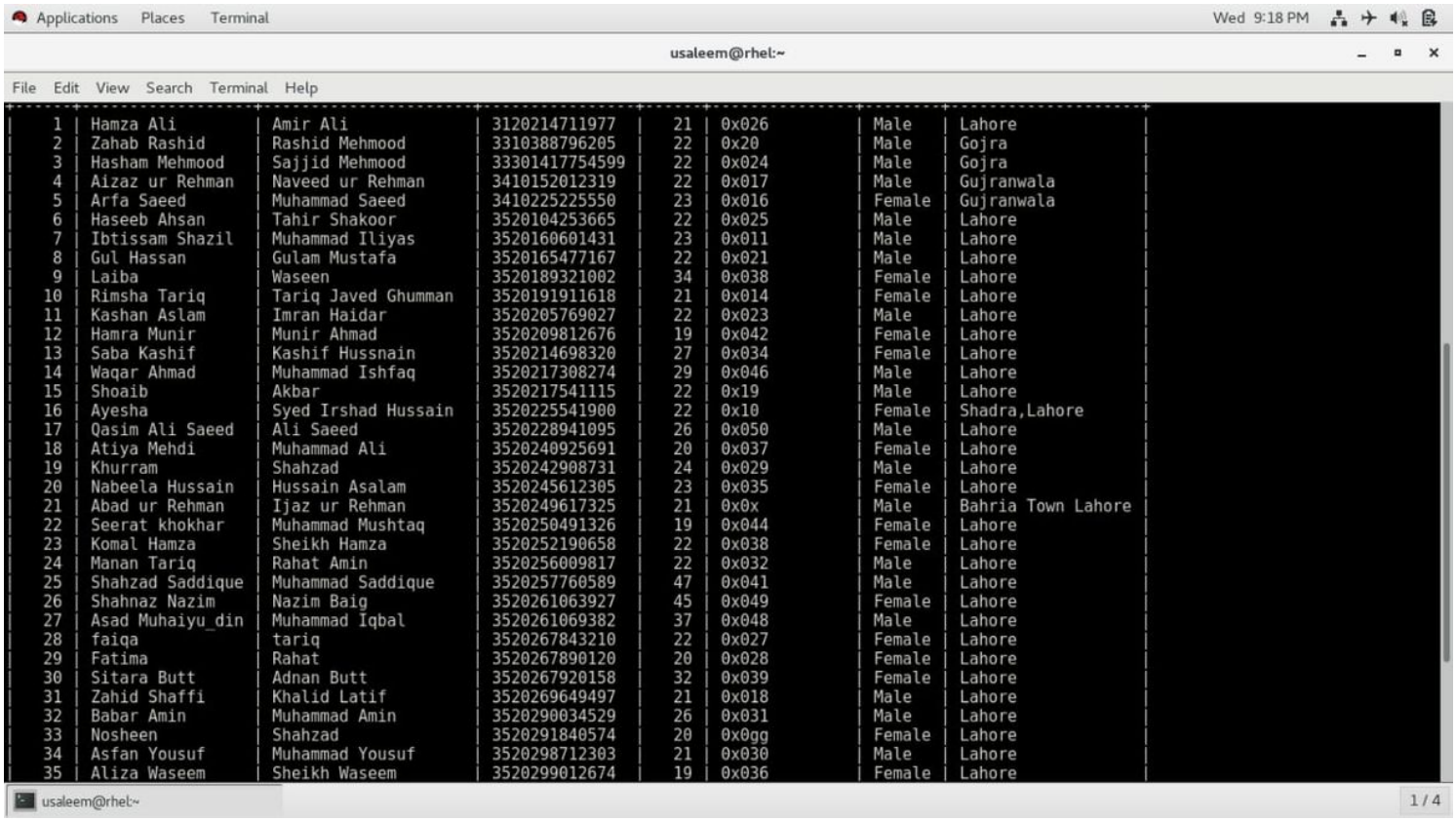

Figure 23

Database

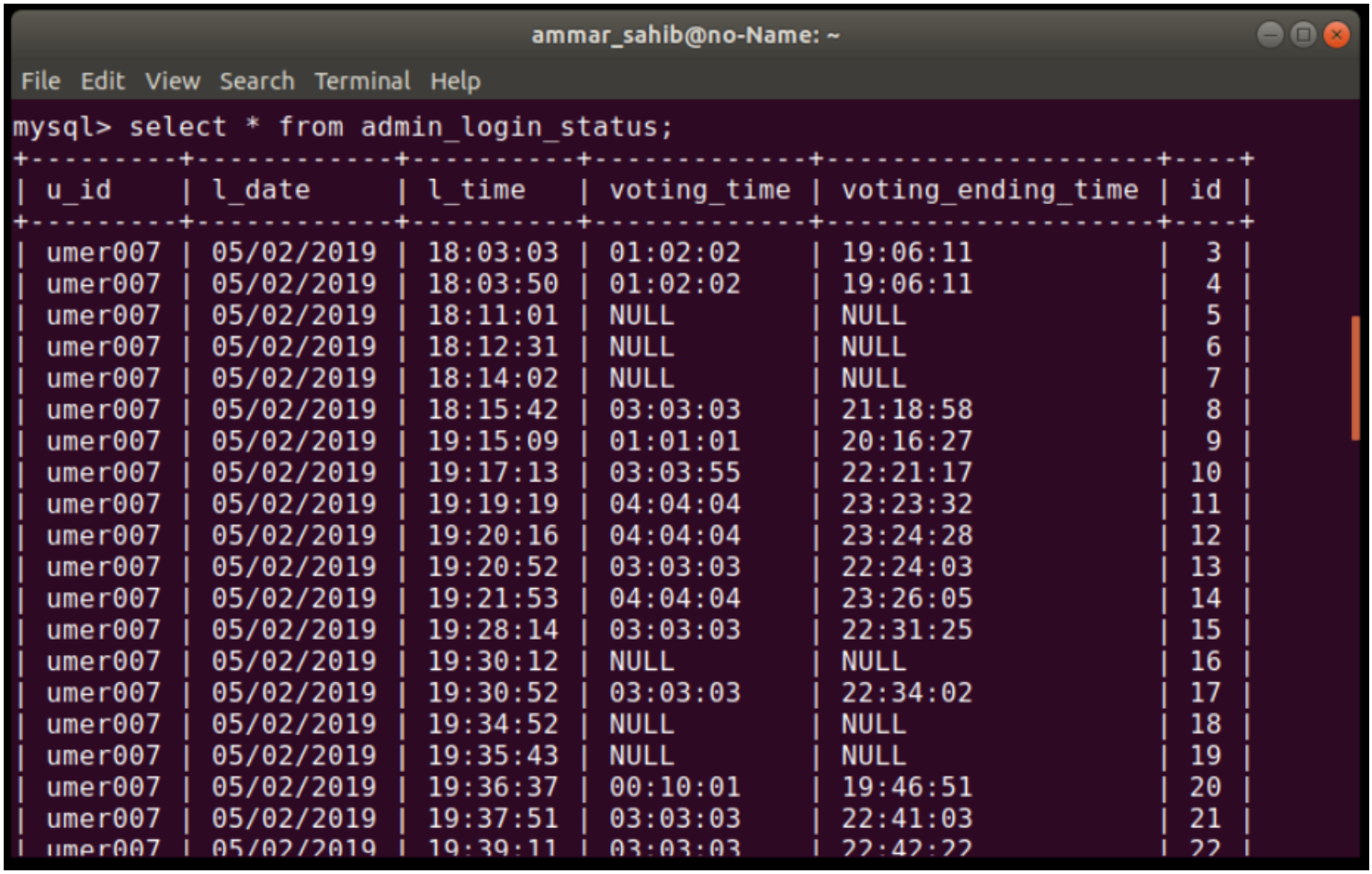

Figure 24

Admin login detail

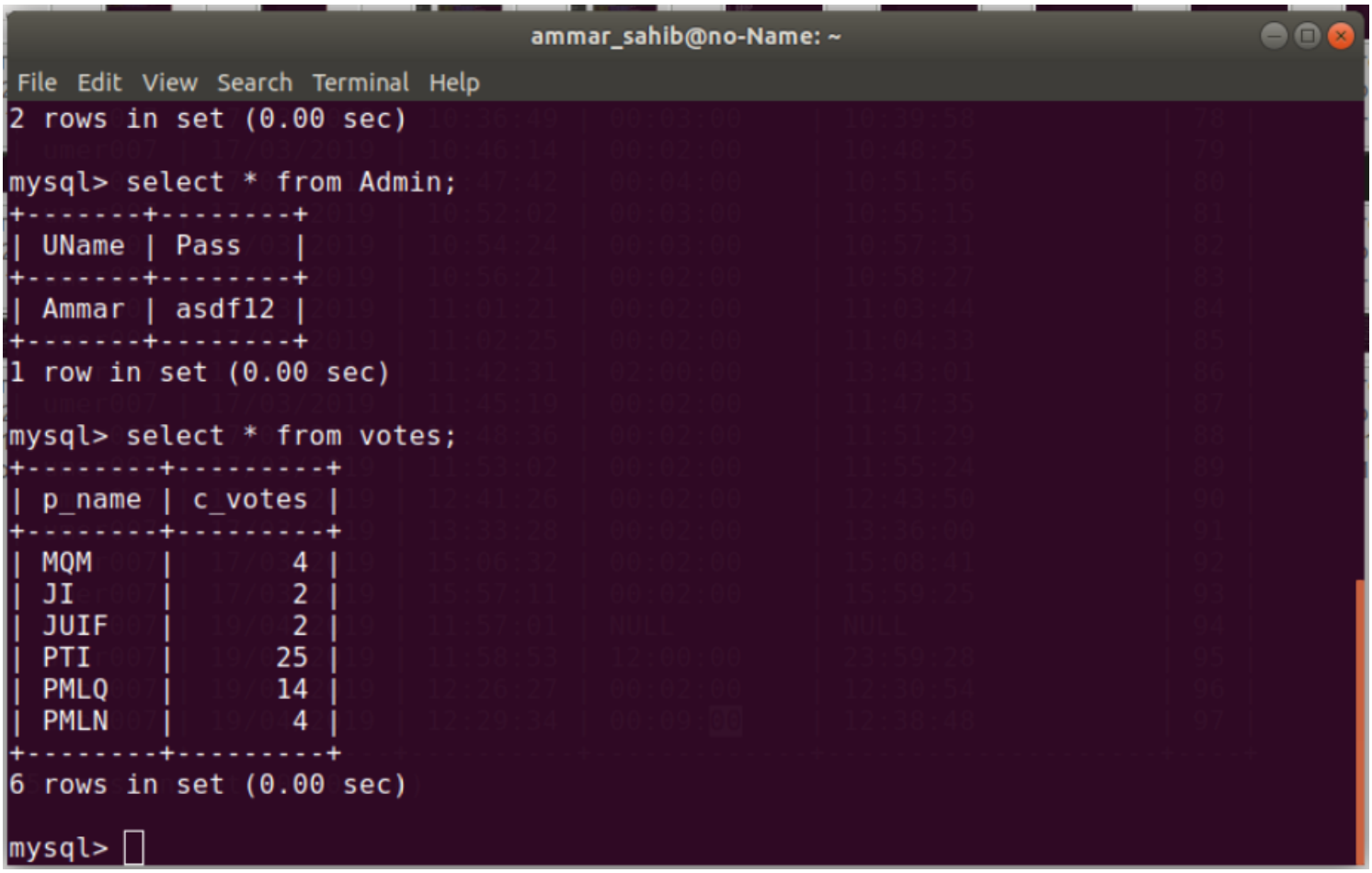

Figure 25

List of selected votes

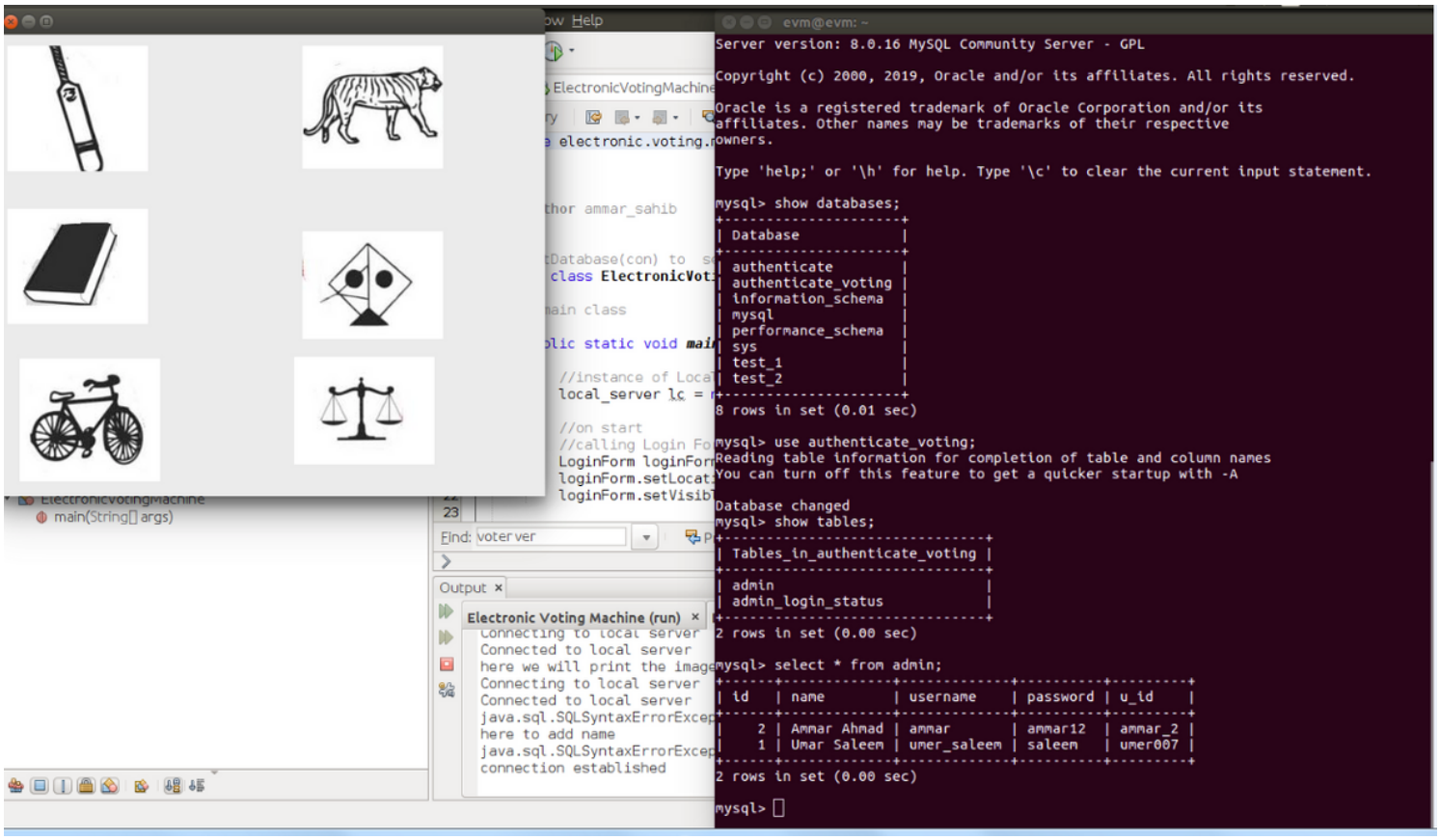

Figure 26

Ballot paper preview

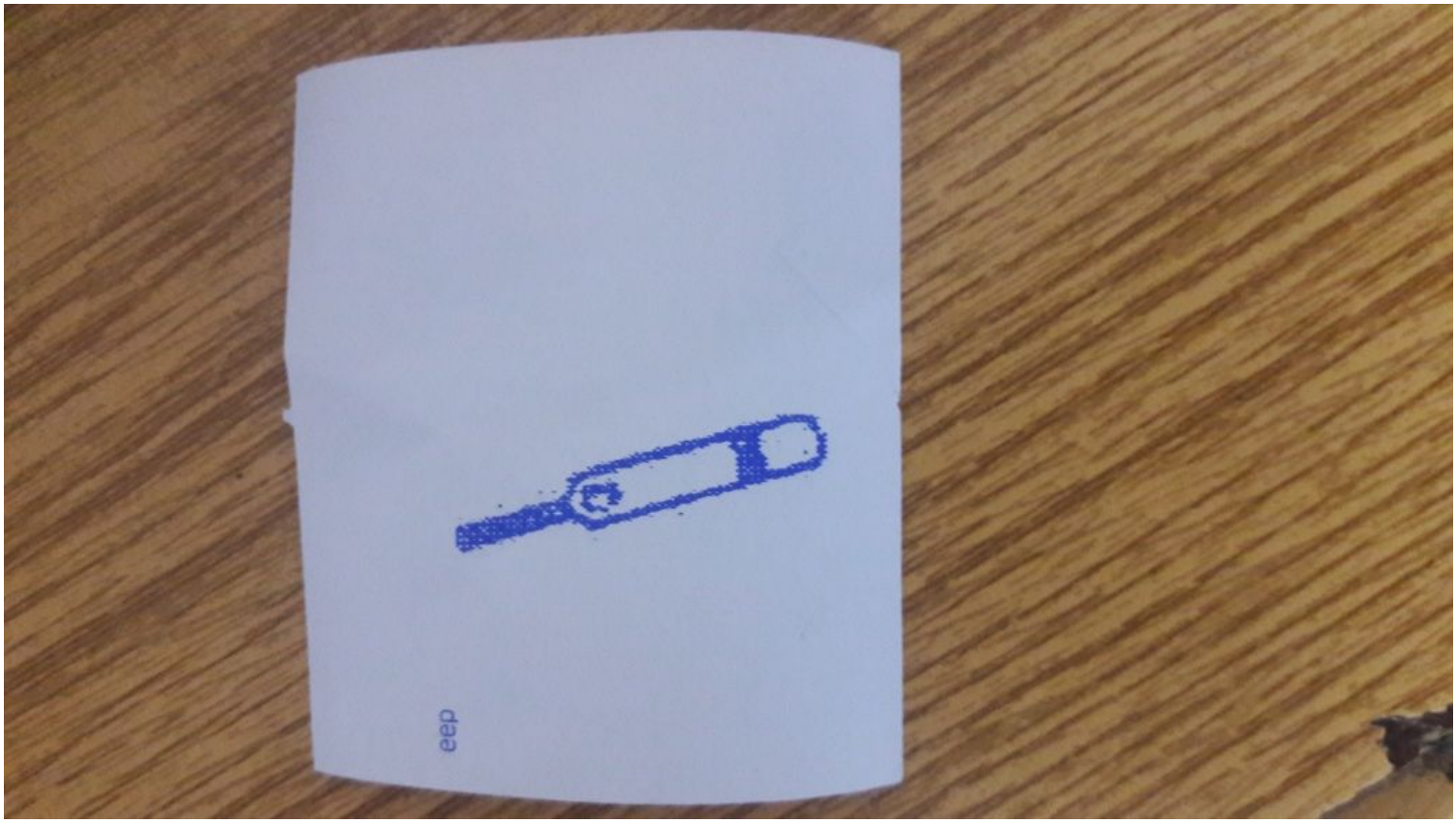

Figure 27

Printed vote