Case Study For Secure Program: ATM, CARD, PIN, Money Withdrawal

- Formulated abuser story corresponding to given threat is

- Threats related to ATM may be: surfing, skimming means identity theft, (**stealing personal information**, such as credit card numbers or login credentials) phishing, denial of service, man in middle attack and traffic analysis.
- Here **our assents are money and user's secret information corresponding to his ATM card and pin number.**

Activate Wind
Go to Settings to

-misuse case and abuser stories...

- During an ATM attack abuser wants to obtain pin number of abuser to get unauthorized access of user's account
- Pin number generation algorithms?

Activate Wind
Go to Settings to

Abuser Story

- An unauthorized user captures identification and authentication of authorized user for stealing money when authorized user taking out money from his account using ATM machine. It can be mitigated by protecting secret information.

Activate Wind
Go to Settings to

Threat Modelling in Software Development Life Cycle

Phases	Threats	
Analysis	• Business goals e.g. allowing 24hrs banking via web can yield DOS • System Boundary assessment: Every legitimate system entry or exit point is a threat, as well as other possibly illegitimate access points to a system. • analysis on abuse of privileges by insiders can yield a lot of threat and vulnerability information	
Design	Input Validation	BOF, XSS,SQLIA, Canonicalization-specific-pattern attack-comput mapping between two inputs with slight change say in hash.
	Authentication	Network eavesdropping, brute force attacks, dictionary attacks, cookies reply, credential theft
	Authorization	Elevation of privilege , disclosure of confidential data, data tampering , luring attacks/urgency cheating –How fish?
	Configuration mgmt	Unauthorized access to administration interfaces ; unauthorized access to configuration store, retrieval of clear text configuration data; lack of individual accountability, over privileged process and service accounts

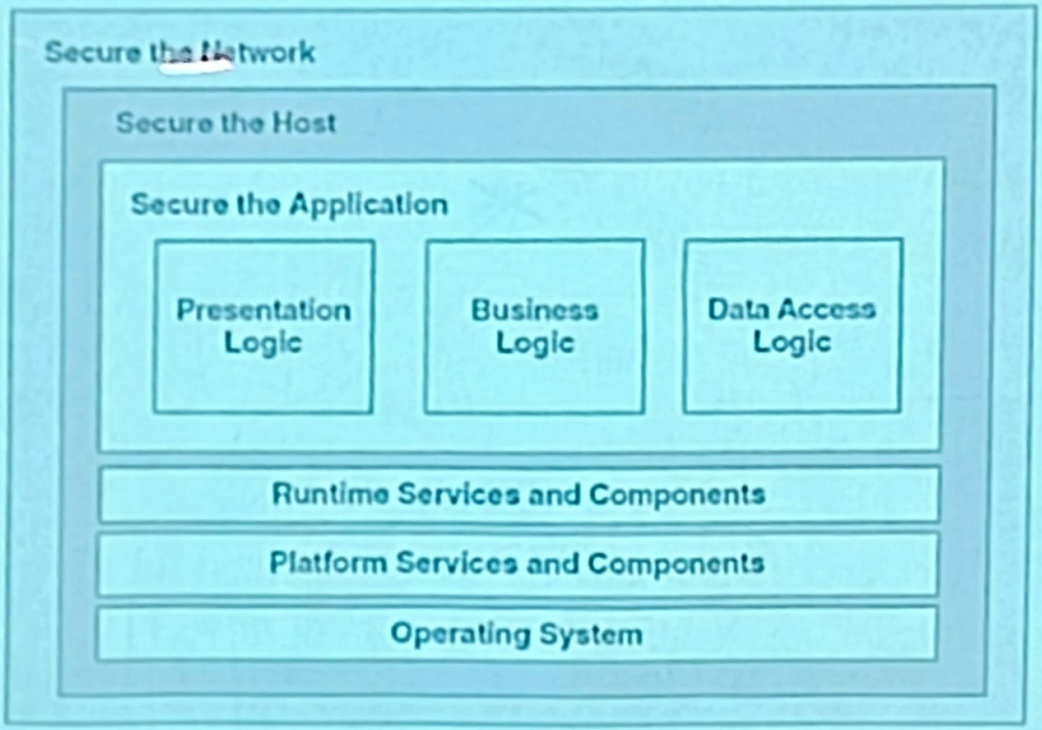
	Sensitive mgmt	Access sensitive data in storage , network eavesdropping , data tampering
	Session mgmt	Session hijacking, session replay, man in the middle
	Cryptography	Poor key generation or key mgmt, weak or custom encryption
	Parameter manipulation	Query string manipulation , form field manipulation, cookie manipulation , HTTP header manipulation
	Exception mgmt	Information disclosure, denial of service
	Auditing & logging	User denies performing an operation; attacker exploits an application without trace, attacker covers his or her tracks

Activate Wind
Go to Settings to

Development	Input Validation	BOF, XSS,SQLIA, Canonicalization
	Authentication	Network eavesdropping, brute force attacks, dictionary attacks, cookies reply, credential theft
	Authorization	Elevation of privilege, disclosure of confidential data, data tampering, luring attacks
	Configuration mgmt	Unauthorized access to administration interfaces; unauthorized access to configuration store, retrieval of clear text configuration data; lack of individual accountability, over privileged process and service accounts
	Sensitive mgmt	Access sensitive data in storage, network eavesdropping , data tampering
	Session mgmt	Session hijacking, session replay, man in the middle
	Cryptography	Poor key generation or key mgmt, weak or custom encryption
	Parameter manipulation	Query string manipulation, form field manipulation, cookie manipulation, HTTP header manipulation
	Exception mgmt	Information disclosure, denial of service

Testing	Improper test data: Most published literatures introduce techniques for generating test cases from UML models, such as sequence diagrams or activity diagrams, and so on. Any diagram-based test method is based on path traversing. A run driven by one test case may not detect the modelled threats, so various runs taking different paths may be necessary to find a path which can activate the threat behaviour. Killing criteria should get defined properly.	
Deployment	Network Threats	Information gathering
		Sniffing or eavesdropping
		Spoofing
		Session hijacking
		Denial of service, probing, R2L, L2R
	Host Threats	Viruses , Trojan horse and worms
		Foot printing
		Password cracking
		Denial of service
		Arbitrary code execution
		Unauthorized access
Maintenance	Improper update of database , Digital Forensic analysis	

The Holistic Approach



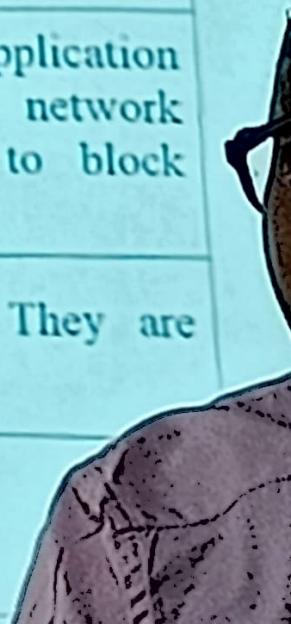
- Web application security must be addressed across application tiers and at multiple layers.

- An attacker can exploit weaknesses at any layer. For this reason, the we discuss here a holistic approach to application security and applies it at all three layers.

Activate Windows
Go to Settings to

Network Security Tools

Element	Description
Router	Routers are your outermost network ring. They direct packets to the ports and protocols that you have prepared your applications to work with. Insecure TCP/IP protocols are blocked at this ring.
Firewall	The firewall blocks those protocols and ports that the application does not use. Additionally, firewalls enforce secure network traffic by providing application specific Filtering to block malicious communications.
Switch	Switches are used to separate network segments. They are frequently overlooked or over trusted.
IPS	Intrusion Protection systems



CASE STUDY 1 :National level conference at dept of computer engg, VJTI When we begin to think about the problem of automating an INTERFACE 95 VJTI Conference organized by ACE under the chairman ship of Dr. Bandu Meshram, (ACE Chairman), Dr. Lalita Deshpande (ACE Treasurer) and ask "what information is important to conference organizers?". We might talk with a few people, look at various records created at previous conferences, and come to the conclusion that information about papers, tutorial, authors and the such are important to understand. The information model shows the information that we discovered: we have "a paper is composed of a title and references to some number of authors and ....". The sponsorship was obtained from various industries. The inauguration was made by Dr Srinivasan Ramani (Founder Director of NCST Mumbai and Hewlett Packard Labs India) and experts invited were Dr.G. Shivkumar and Dr. Chaudhary IIT Powai for the paper presentation and software contest.

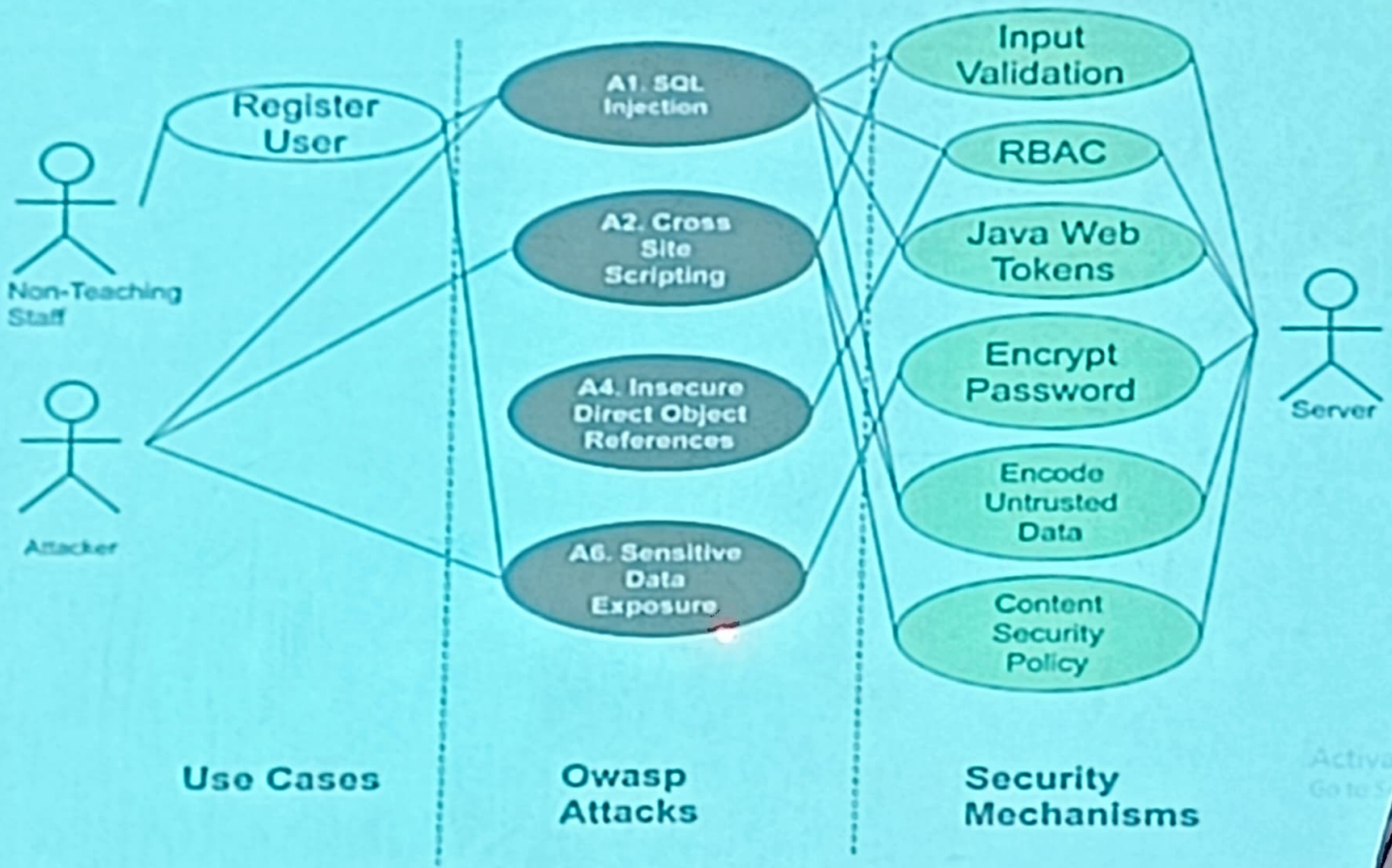
Q1 .Construct DFD, and algorithms for distribute paper process and data dictionary for data stores- collectionOfPapers.

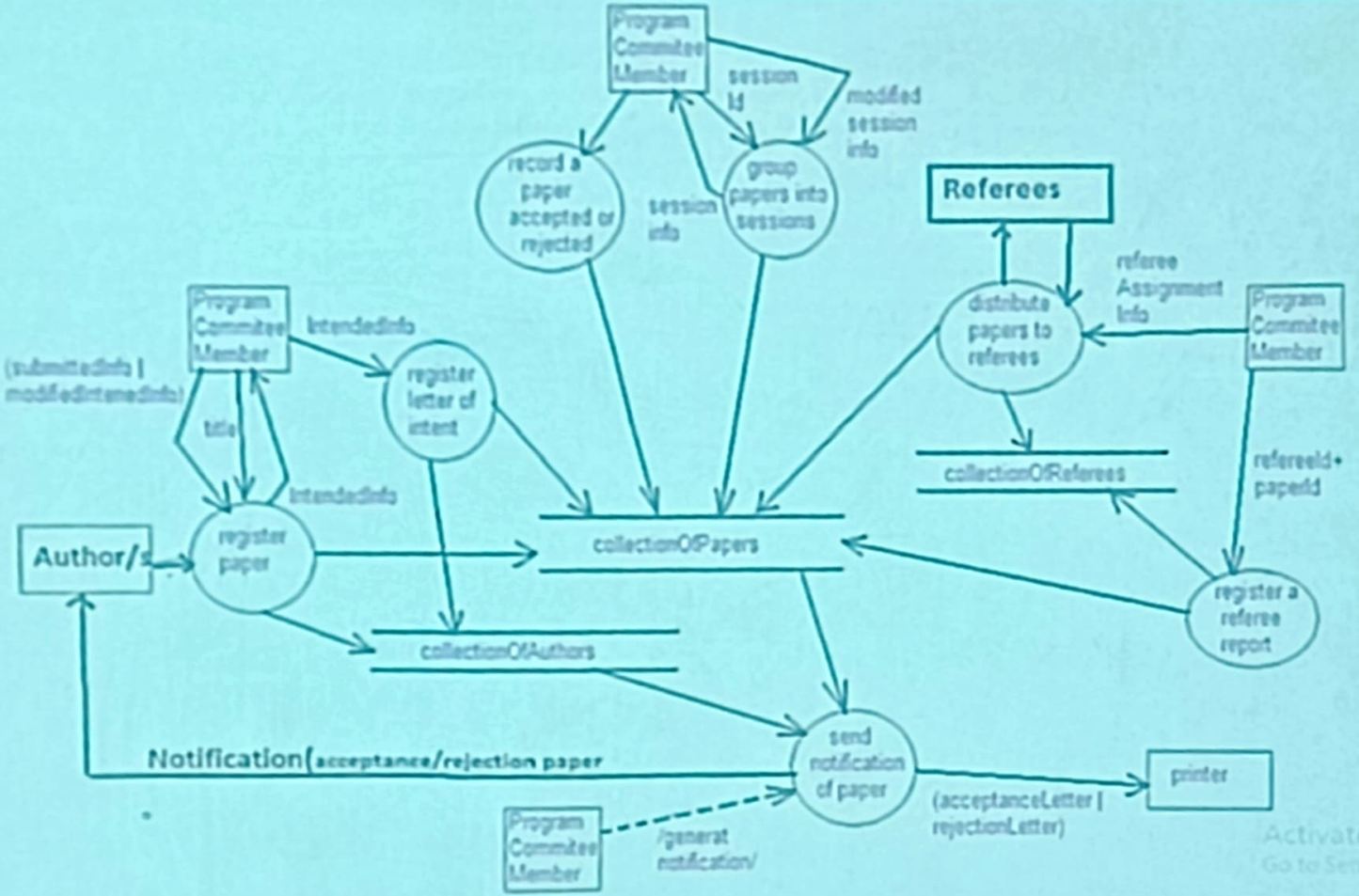
How can you use the secure software clife cycle for the implementation and deployment of the program

Activate Wind
Go to Settings to

Misuse case

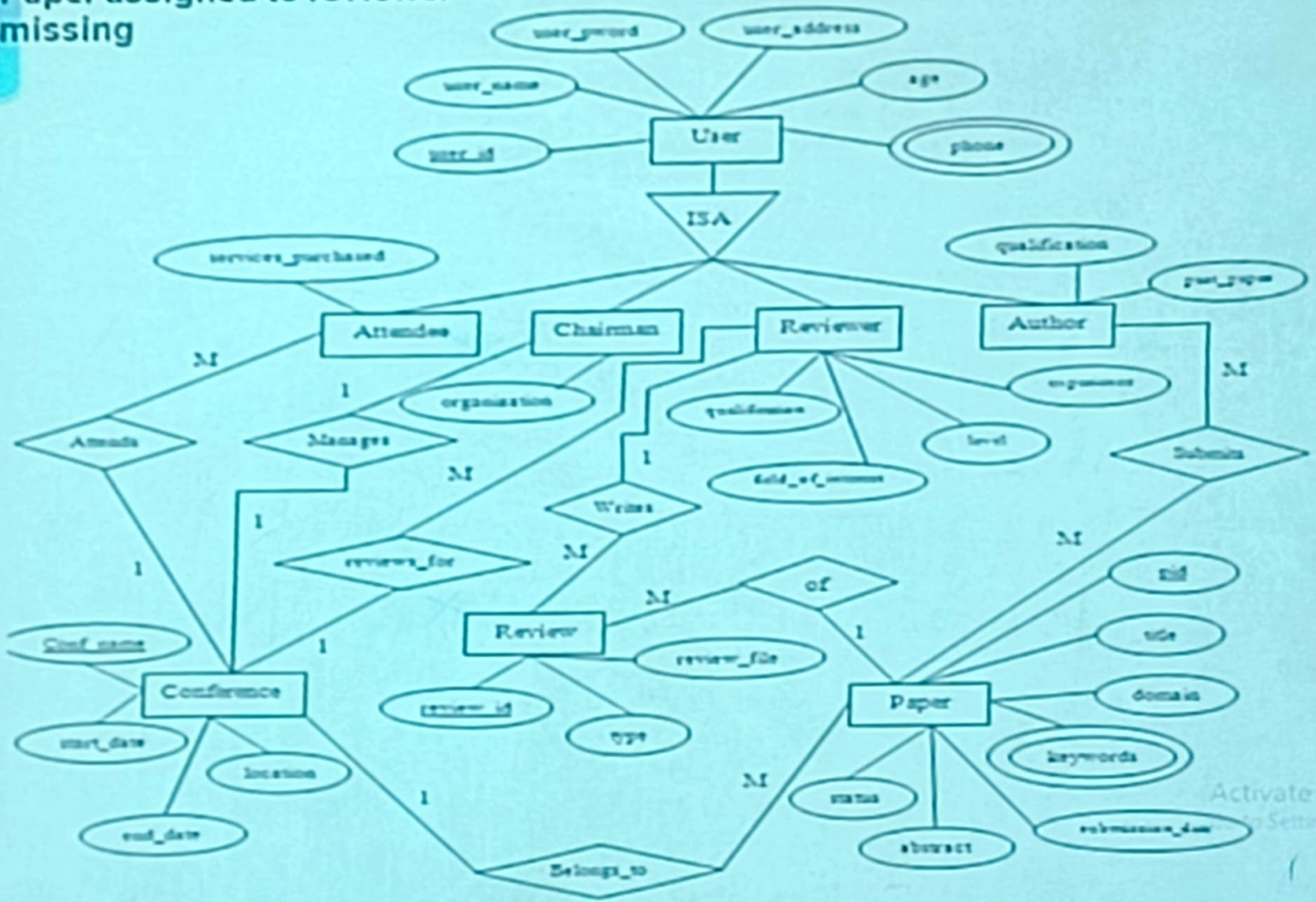
:Basic Knowledge Requirement-use cae, misuse case(ATTACK), Security Mechanism





Activate Wind
Go to Settings to

Paper assigned to reviewer-missing



Analysis of Web Based Conference Management System for security

The *analysis phase* answers the questions of *who* will use the system, *what* the system will do, and *where* and *when* it will be used. An analysis strategy is developed to guide the project team's efforts.

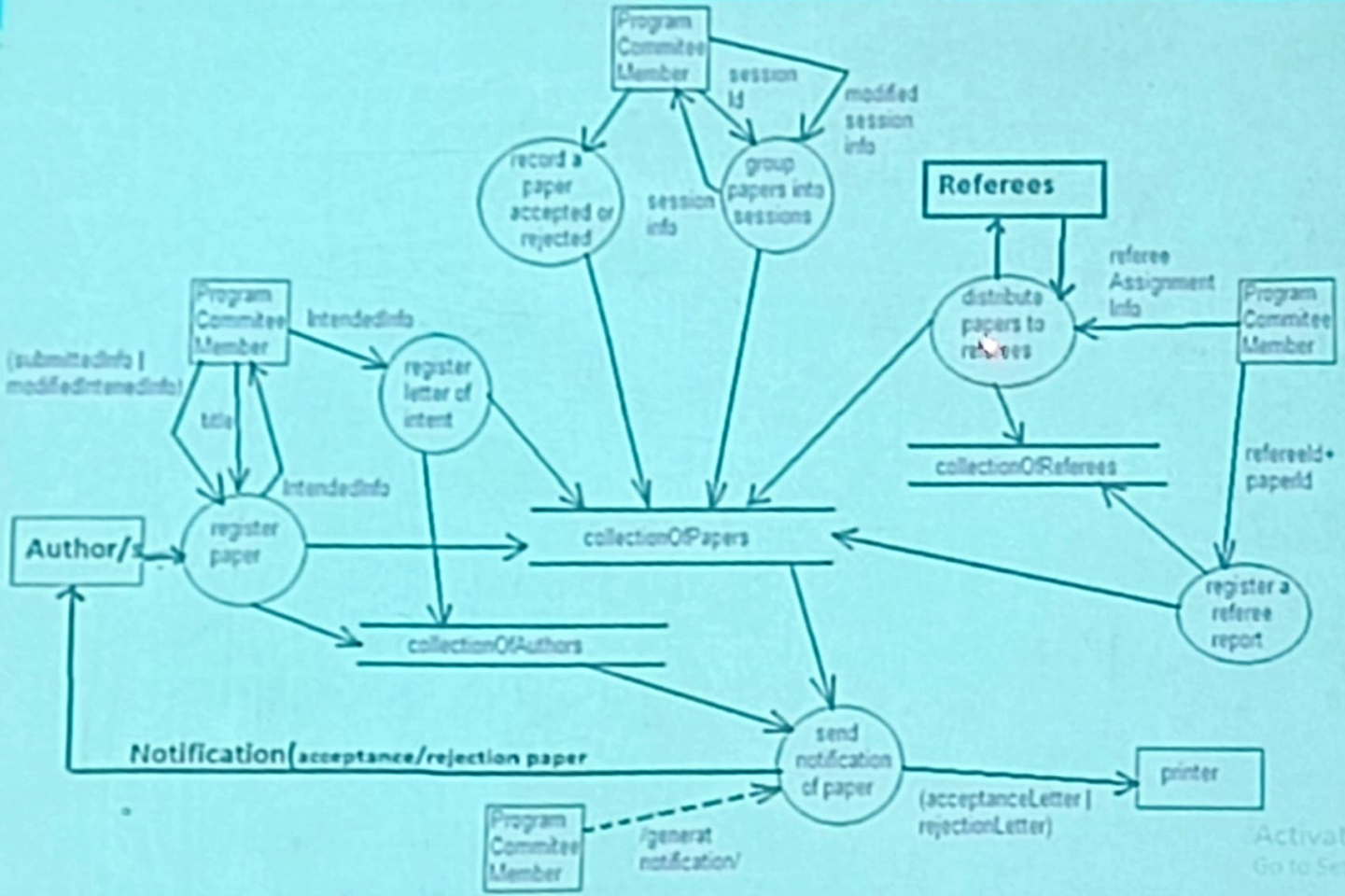
Such a strategy usually includes an analysis of the current system (called the as-is system) and its problems, and then ways to design a new system (called the to-be system).

Security provision against Threats in Software Development Life Cycle

Phases	Threats	
Analysis	• Business goals e.g. allowing 24hrs payment of fees via web can yield DOS • Privileges can be given to convenor and organiser account only so that anyone else can not misuse those privileges.	
Design	Input Validation	During designing of online form do proper validation of name, email, comment section, abstract section, file upload etc. Other wise this sections can be used by attacker for input validation.
	Authentication	Only authorised user should get access to website otherwise hacker can perform any of the following activity Network eavesdropping, brute force attacks, dictionary attacks, cookies reply, credential theft . Biometric security finger , face , iris etc.

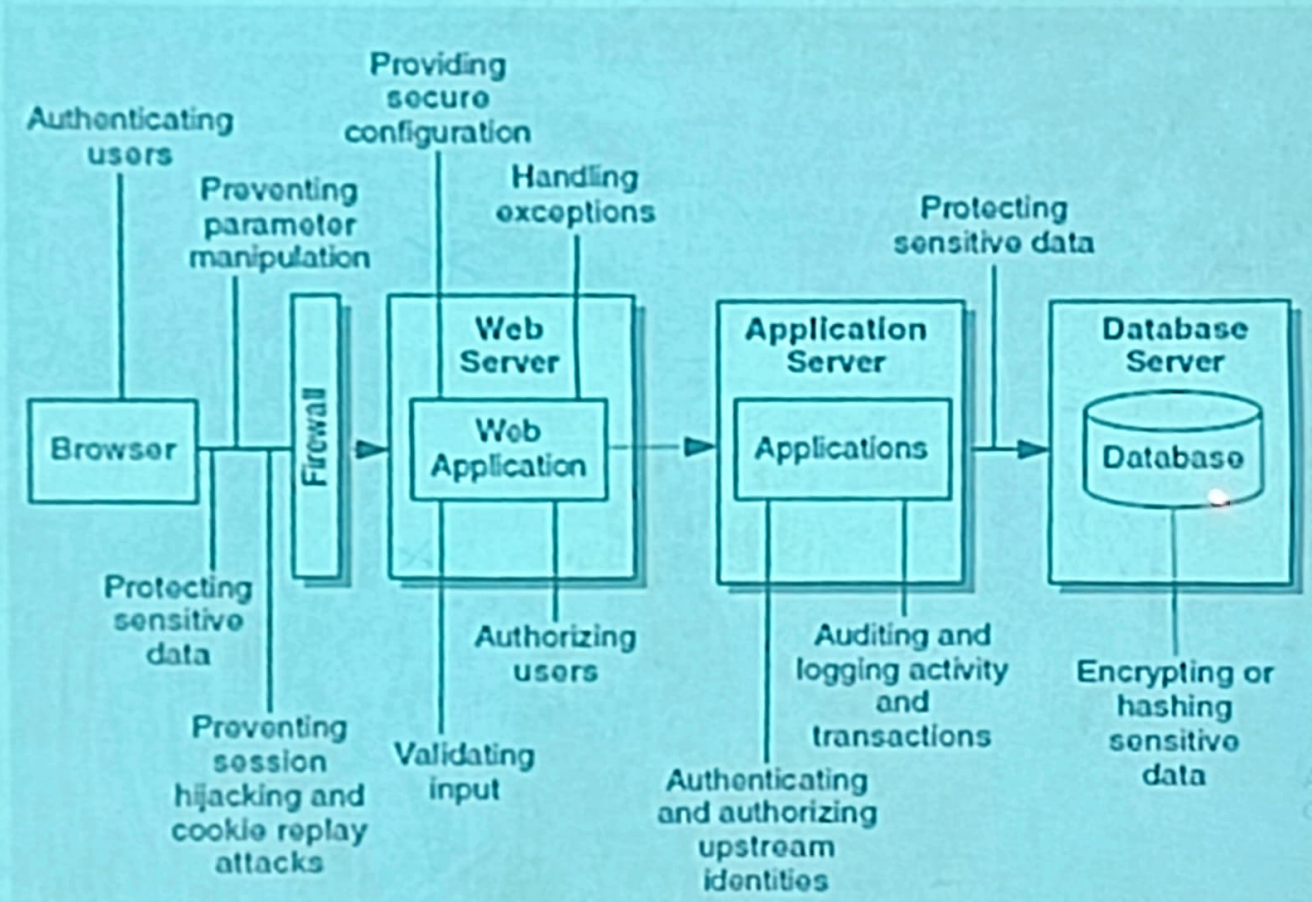
	Authorization	Identify all roles (admin, convenor, organiser, reviewer) properly then give privileges according to the roles.
	Sensitive mgmt	Access to sensitive data like payment details, papers should be given to convenor and organisers only, other wise their is possibility of network eavesdropping , data tampering.
	Session mgmt	Once the user login till that user is going to logout his session should get maintain properly.
	Cryptography	For sorting password in database we need encrypted password so keys for encryption and decryption should be strong so that password will get revel. Submission of paper and paper fee payment through cryptography and digital signature
	Parameter manipulation	Parameters passed by clients like login name, password, email should be manipulated properly by removing suspicious special characters.
	Exception	Error should get handled properly, it should not

Implementation	Input Validation	Validate all text boxes, remove special characters like < , >, from otherwise SQLIA,XSS and BOF is possible
	Authenticatio n	Instead of using only login name and password use 3D password otherwise hacker can get access to your database.
	Authorization	Identify all roles (admin, convenor, organiser, reviewer) properly then give privileges according to the roles. Make proper use of grant command.
	Sensitive mgmt	Access to sensitive data like payment details, papers should be given to convenor and organisers only , otherwise there is possibility of network eavesdropping , data tampering
	Session mgmt	Once the user login till that user is going to logout his session should get maintain properly using Http Session Objects or any other session tracking technique. Otherwise attacker hijack any session.

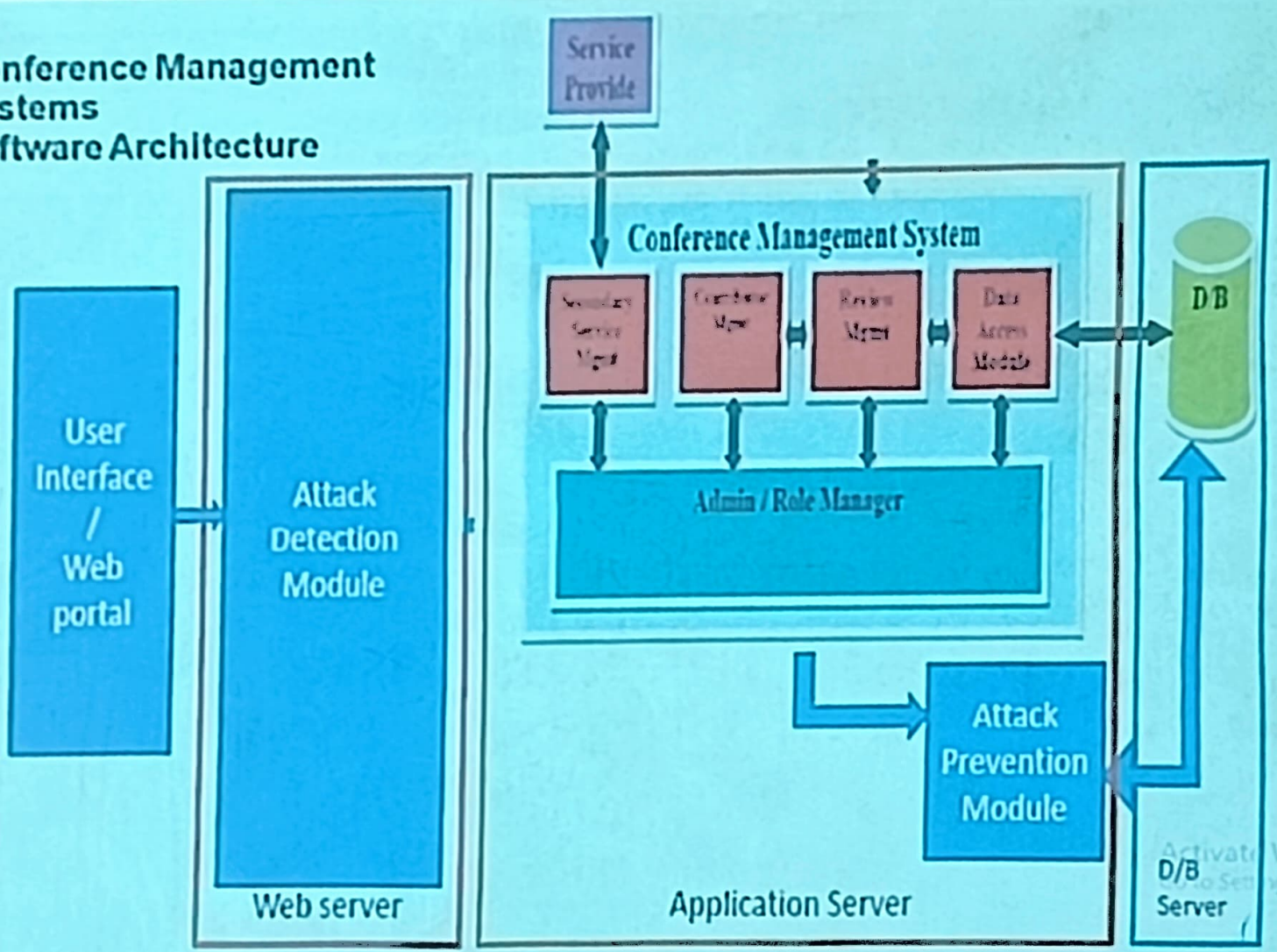


Activate Wind
Go to Settings to

Eliminate Web application design issues



Conference Management Systems Software Architecture



Voting Machine Security

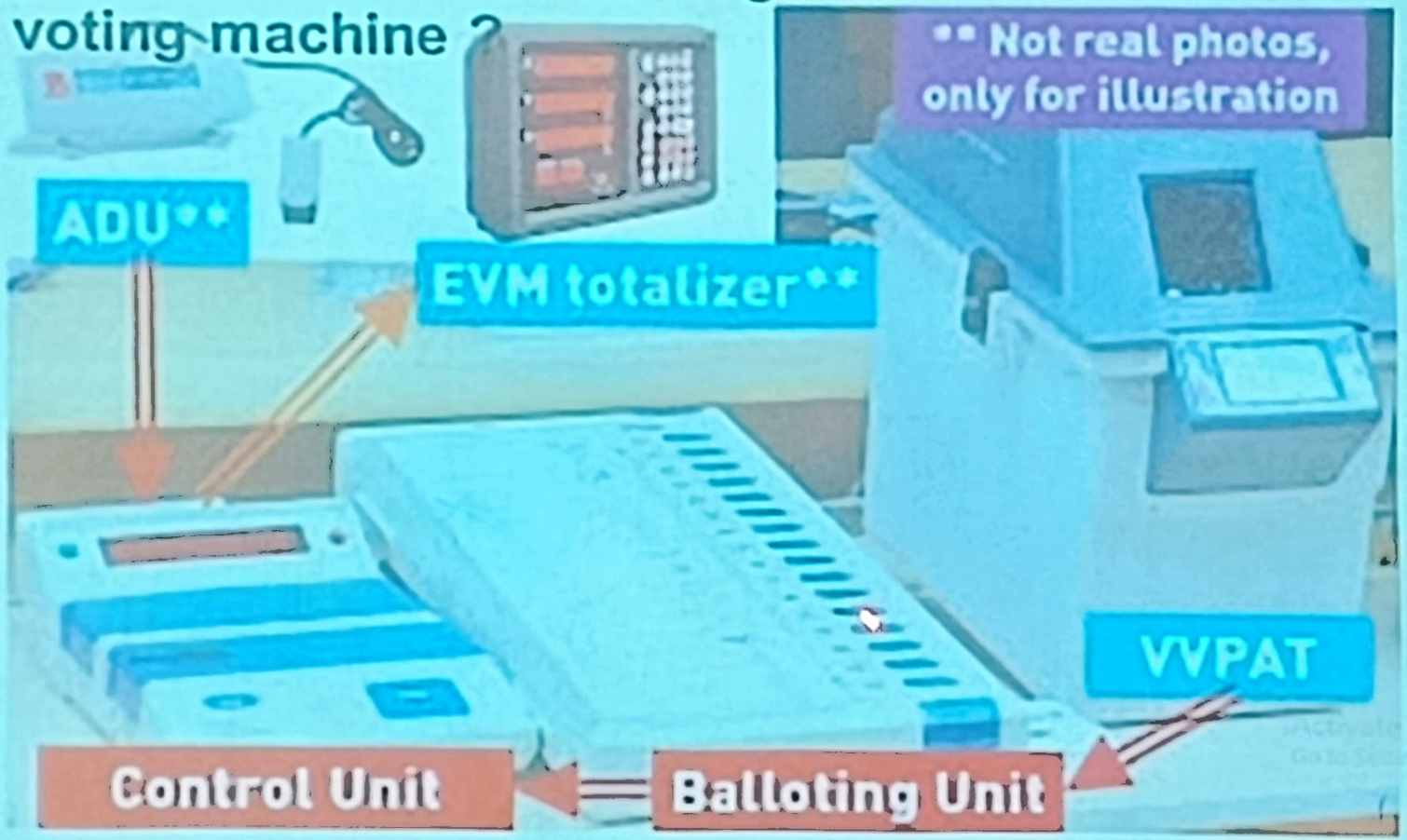
Give the process chart for the design of electronic voting machine ?

ALGORITHMS USED.

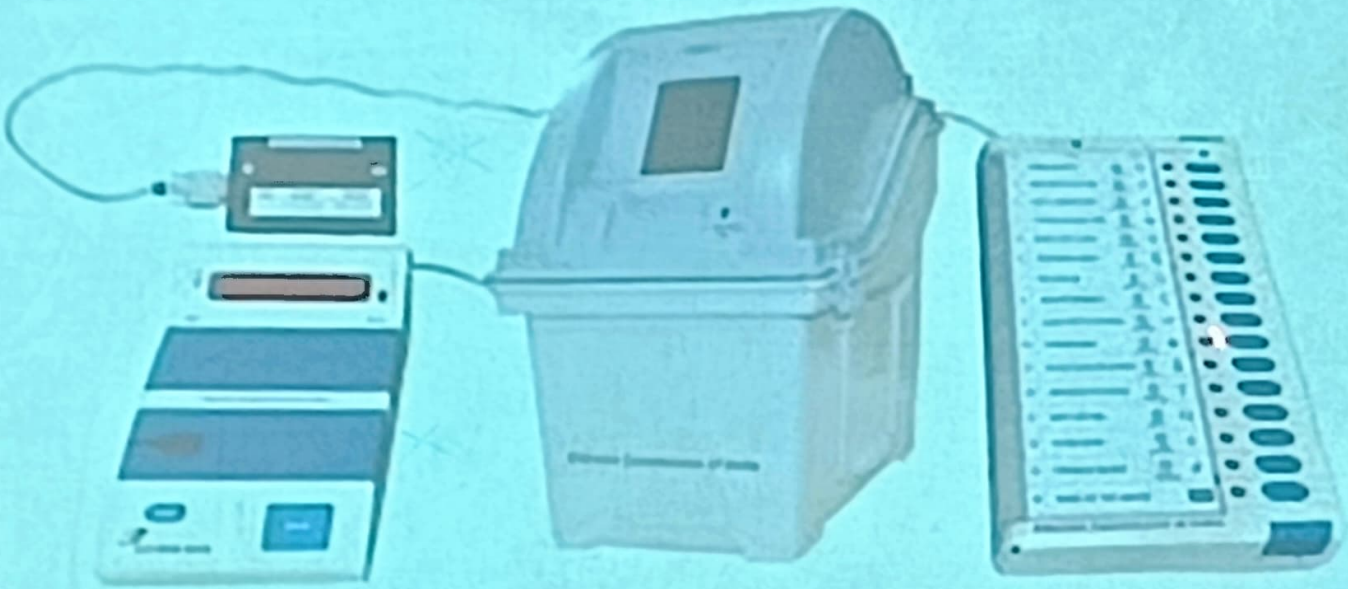
Q1 Several countries in the world – including Germany, Netherlands and the United States of America – have banned the use of EVMs. Is there any issue of security design , information security or physical security, cyber crime or any other issue.? Justify your observation with reason.[10]

Activate Windows
Go to Settings to

Give the context level DFD and 1 level process chart for the design of electronic voting machine ?

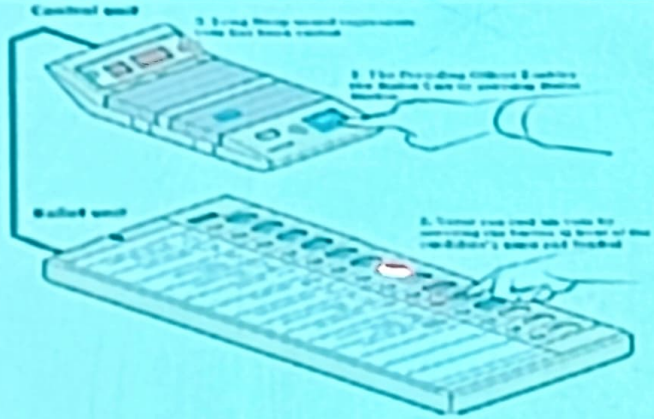


GUI DESIGN OF EVM

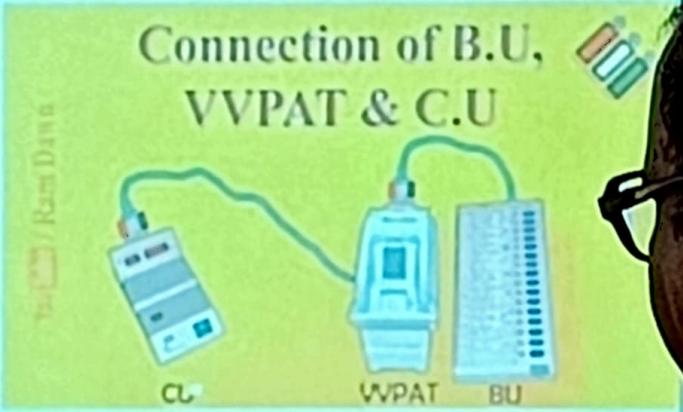


ALGORITHM TO PRINT THE VOTER SLIP

"Truth can only be found in one place: the code."
— **Robert C. Martin,** Clean Code: A Handbook of Agile Software Craftsmanship



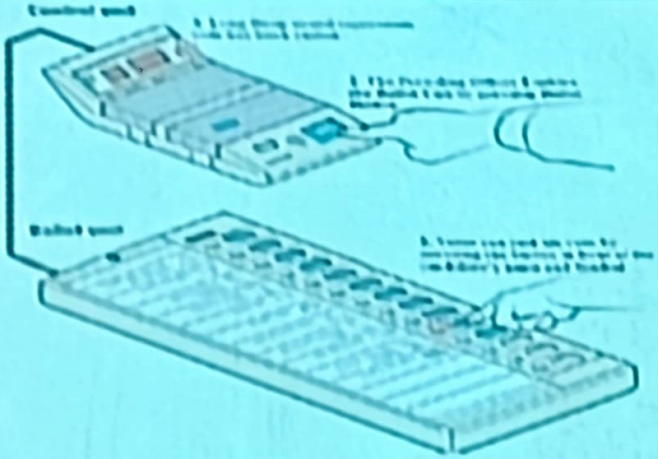
BU is connected to VVPAT and VVPAT is connected to CU.



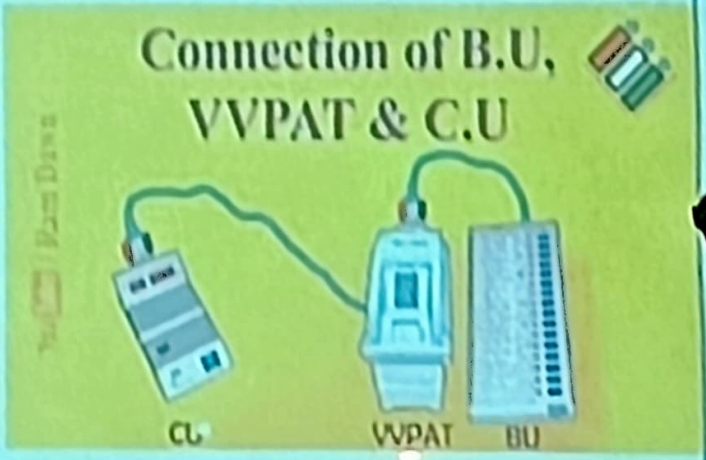
Items of EVM

-ALGORITHM TO PRINT THE VOTER SLIP

"Truth can only be found in one place: the code."
— **Robert C. Martin,** Clean Code: A Handbook of Agile Software Craftsmanship



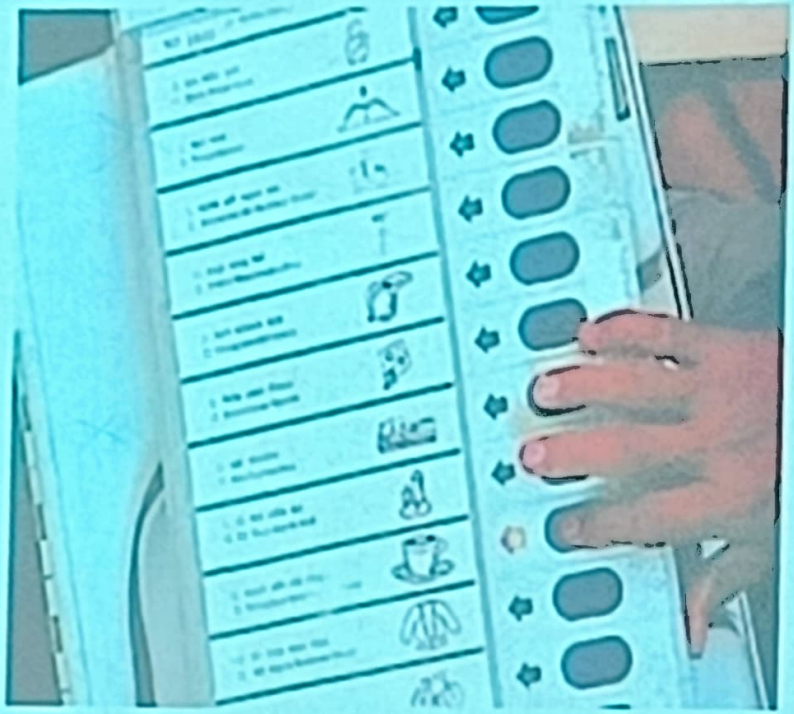
BU is connected to VVPAT and VVPAT is connected to CU.



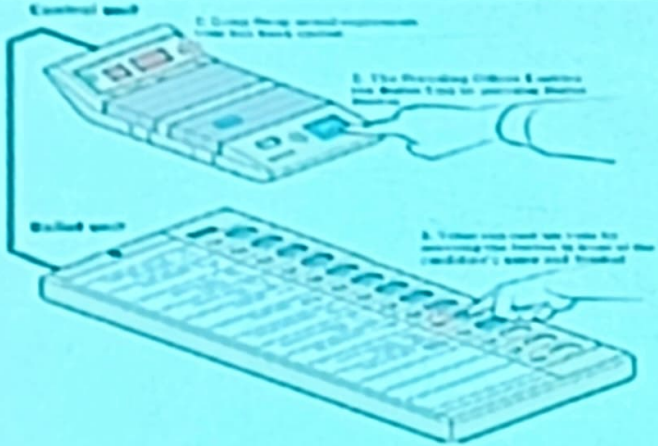
Items of EVM

Modifications for Security:

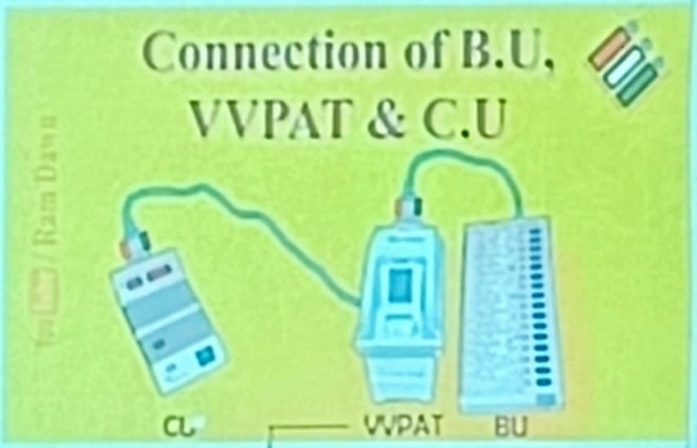
GUI DESIGN-put camera on machine for physical security



Position of VVPAT after CU as printer in Computer



BU is connected to VVPAT and VVPAT is connected to CU.



Items of EVM

calculate slips, vvpat after processing by CU- CHANGE DESIGN

Assembly be packed while in custody and counting

- No internet connectivity/no mobile with people

Faraday bag or airgapped systems to isolate from radio frequency signals, including wi-fi, blue tooth or electromagnetic interferences from mobile , laptops.

- Total Machine Count In India-send to booth count. Voting in camera.
- Count slips and machine votes.

Activate Winc
Go to Settings to