**Defending against advanced attack vectors on Biometric Identification and Authentication Systems**

**1. Succinctly explain your understanding of the Problem Statement.\***

Biometric recognition offers a promising approach for security applications, with some advantages over the classical methods like passwords, PIN etc. The reason is a biometric cannot be forgotten, lost or stolen and it is easy to check if one person has several identities.

However, biometric breaching using imitation of behavioral attributes like digital signatures; image or video recording; brute-forcing or hacking over the WAN or fetching the decryption key from the transmission media while doing net banking or online-financial transactions etc. have given the malicious users access to sensitive information  including bank-account numbers and  even our own biometrics like fingerprints, face, hand palms etc. which can be exploited in numerous ways.

Our target is to secure money transactions that take place using ATMs using Biometric Security as well as protecting the transactions from **Biometric Breaches**.

Every ATM is susceptible to the following breaches:

**A. Fake ATMs :-** A fake ATM is a machine which is similar to genuine machines. Attackers may install it in place of genuine machines. Nowadays, users cannot authenticate at the ATM. If a user uses this machine then, definitely he would share all his account information including PIN. No doubt it is a big threat but in India, it is a very typical task to perform. In the survey we have not found any case of this type.

**B. Shoulder Surfing:-** Through a video camera or directly, it is possible for an attacker to know the PIN. It is easier to know at a merchant's machine where a user gives to the ATM card for payment and video cameras capture a video for the same. Sometimes using skimming machines, attackers can record all account information and forge an ATM card.

**C. Skimming Devices:-** The skimming devices can be attached with ATM machines and steal data from multiple ATM cards. Mostly this type of attack is to be done at merchant’s machine

where the user gives an ATM card for payment purposes. In the survey, Reserve Bank of India reports said that this is very common and threatening in India for many years.

**D. Fake keypad-overlay attack**:- Attacker may place a fake keyboard overlay upon a real keypad. Then this fake overlay stores pressed keypad buttons with time. This information can be used to compromise PIN. Now it is easy for an attacker to use an ATM card of any user.

**E. Criminal Forcing-** A Criminal forcing an innocent to go to the ATM Booth to withdraw money and give it to the criminal standing outside.

So, our aim is not only securing the transactions from the above listed breaches but also improvising on the existing technologies used in ATM transactions.

**2. What is the research & development work that has already been done in this area? (Both Globally & India)\***

The research and development works are given in the following links :

1. ATMs with biometric and wavelet based AES.

The basis of solving our problem is based on this research paper.

<https://www.matec-conferences.org/articles/matecconf/pdf/2016/05/matecconf_iccma2016_06003.pdf>

1. Securing banking communication between bank database and ATMs using TLS Handshake

<https://pdfs.semanticscholar.org/457e/6d60bb5f90ab0037f959886a4fd24eef1fb6.pdf>

1. Reliability of ATM Protocols and Designing a New One

<https://www.researchgate.net/publication/273260669_A_Reliable_ATM_Protocol_and_Comparative_Analysis_on_Various_Parameters_with_Other_ATM_Protocols>

      4.   Enhancing Banking Security Features of an ATM

<https://shodhganga.inflibnet.ac.in/bitstream/10603/25038/9/chapter-5.pdf>

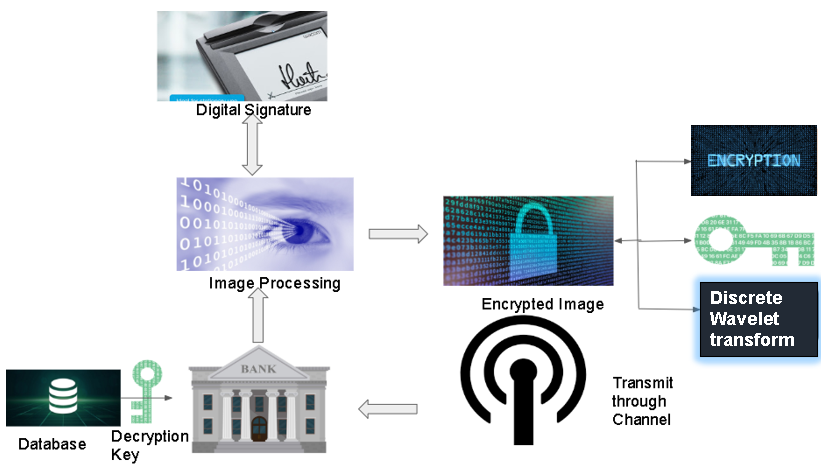
      5.   Biometric ATMs in <https://www.biometricupdate.com/201901/japanese-bank-introducing-biometric-atms-to-open-accounts>

**3. Briefly describe how you approach solving the problem statement. (You may use flow charts & diagrams) \*.**

The 4 Digit PIN is easy to crack using dictionary attack , thermal footprinting and many more. The 4 digit pin can be traced easily and therefore, is not secure in this modern era . Moreover, the encryption standard used in ATM machines is DES or Triple DES(a type of computerized cryptography where block cipher algorithms are applied three times to each data block that is repeating DES Algorithm thrice times.) which is currently not secure for transmitting essential information of the user because it is mostly dependent on choice of keys for encryption. In this paper, our approach is to make Triple DES more secure. So, we are eliminating the use of the number pad in ATMs. Our approach is to take a digital pen made of stainless steel coated with CMOS-based capacitive sensors (stainless steel is used so that no stain marks remain on the pen’s body after use) is used and a signature pad is installed in place of the existing number pad. The digital pen is placed in a holder with automatic charging facility with a lock whose working principle is to ensure **deadlock** i.e. the lock will open only when a ATM card is inserted into the machine so that there are no theft activities of stealing the pen. The person trying to gain access will hold the pen and start writing his signature onto the signature pad. While writing, the fingerprint gets recorded by the CMOS-based capacitive sensors[6] and after completing the signature , the signature is recorded.

The parameters of Digital Signature are the pen-position data (x-y points) , the 2-Dimensional pen movement angle, writing time and thus, it gains its uniqueness because people have different styles of writing ,different signatures ,different writing times and different ways of holding the pen. All of these parameters are recorded and it becomes very difficult to imitate all of the attributes simultaneously. On top of that, even if a person manages to write the exact signature ,still access to the ATM would not be granted because his fingerprint would not be able to match with the actual one. The 2-way lock is the hardest combination to crack. Keeping in mind problems like different sizing, different writing times and  different number of points existing in every signature for the same user , we normalise ,resample the data signals and verify data samples using efficient algorithms of Machine Learning.

The digital signature image is cropped, resized and processed on applying first-order 2D-Haar Discrete Wavelet Transform. The processed image is then encrypted using Wavelet Based Triple DES (DATA ENCRYPTION STANDARD) and one of the encrypted keys used is our fingerprint. Then, the final data is sent into the channel and then matching is done with the database of the bank which has the decryption key i.e. our fingerprint (registered while issuing our ATM card) and the other keys .Then, the digital signature is mapped with the signature stored in the database corresponding to our ATM card number and fingerprint. If a match is found then acknowledgment is sent to the ATM machine and the user gains access else he is denied access.

****

**4. What will your innovation focus on? \***

**Application of existing technologies in new areas (combination/ adaptation of existing approaches)**

We are combining two different biometric techniques i.e. Fingerprint (by recording ridges and valleys of our finger) and Digital Signature (behavioral attribute) verification in ATMs.

**Totally disruptive approach (Original/ New Concept):**

Our model is a totally disruptive approach i.e. it is our original idea since we are combining two- way lock technology accomplished using fingerprint and digital signature and modifying Triple DES standard by applying DWT to make our Triple DES encrypted data faster, consuming less power and making it more secure.

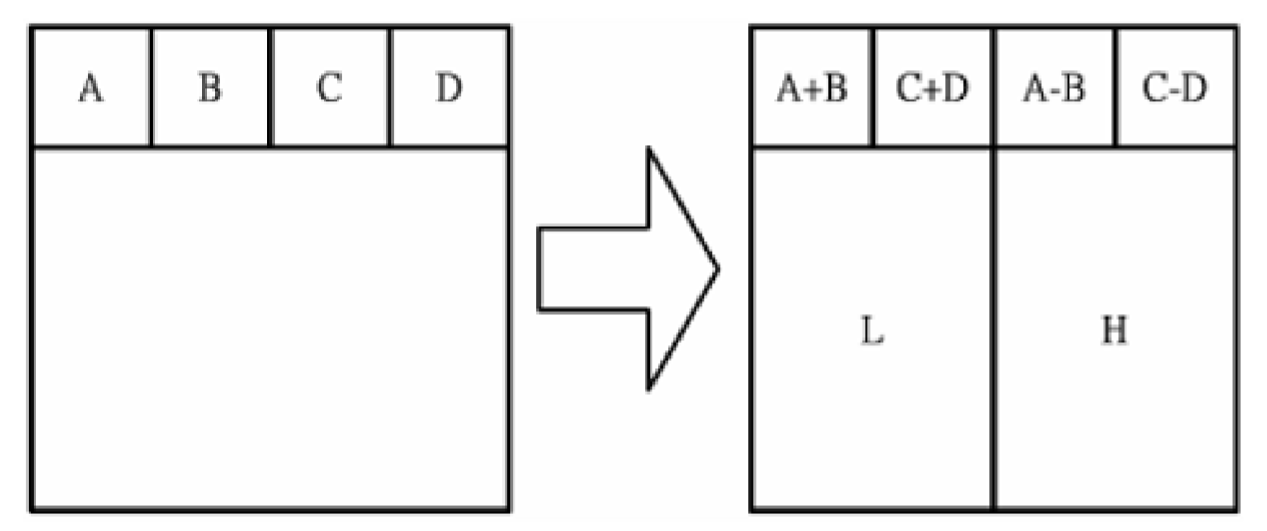
**5. Describe the following regarding your solution:\***

Initially the digital pen is locked in the pen holder. Any attempt to steal the pen will trigger the siren in the ATM Booth. When the user inserts the ATM Card into the card reader , the pen is free to use and the signature pad gets activated which has the token of that pen (i.e. the pen is configured with the pad and no other pen could write on the pad.) and he is now supposed to do the signature. The fingerprint is associated with the card number. In case of **forcing criminal attack**, the user writes “HELP” or “मदद” on the pad. Just like an emergency call aspect in our mobile phones, in the same way, the bank’s and nearby police’s control room would get alerted about this activity and information like the user's card number which was read by the ATM machine and the ATM Booth location will be sent. Accordingly, necessary action against the activity will be taken.

Normally, the user is supposed to write his/her signature on the pad. On writing the signature, parameters like pen-position data (x-y points) , the 2-Dimensional pen movement angle, azimuthal angle and writing time will be recorded. The data signals will then be normalised and resampled using efficient algorithms in Machine Learning.The image will be cropped and resized. After writing the signature, the image will be processed on applying first-order 2D Haar Discrete Wavelet Transform in the following way:

 A 2-dimensional Haar-DWT  consists of two operations: One is the horizontal row operation and the other is the vertical row operation. Detailed procedures of a 2-D Haar-DWT are described as follows:

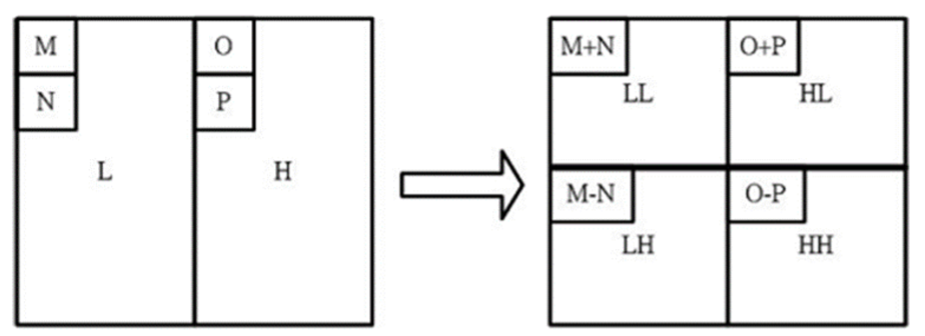
**Step 1:** At first, scan the pixels from left to right in a horizontal direction. Then, perform the addition and subtraction operations on neighboring pixels. Store the sum on the left and the difference on the right as illustrated in Figure 1 below.



**FIGURE 1:       HORIZONTAL ROW OPERATION**

Repeat this operation until all the rows are processed. The pixel sums represent the low frequency part (denoted as symbol L) while the pixel differences represent the high frequency part of the original image (denoted as symbol H).

**Step 2:** Secondly, scan the pixels from top to bottom in a vertical direction. Perform the addition and subtraction operations on neighboring pixels and then store the sum on the top and the difference on the bottom as illustrated in Figure 2.



**FIGURE 2:       VERTICAL OPERATIONS**

Repeat this operation until all the columns are processed. Finally we will obtain 4 sub-bands denoted as LL, HL, LH, and HH respectively. The LL subband is the low frequency portion and hence looks very similar to the original image.

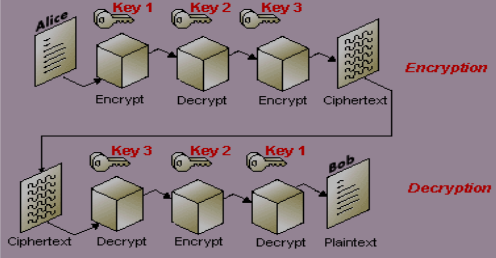
The final output will be similar to Figure 3.



**FIGURE 3**

The processed image is converted to **binary format**.

Prerequisite is Triple DES Encryption and it's working is as listed below.



**FIGURE 4 : TRIPLE DES ENCRYPTION / DECRYPTION**

**DES ALGORITHM:** It is the most widely used symmetric key cryptographic method. It uses a fixed length, 56-bit key and an efficient algorithm to quickly encrypt and decrypt messages.It can be easily implemented in the encryption and decryption process even faster. In general, increasing the key size makes the system more secure. A variation of DES, called Triple-DES uses three applications of DES and two independent DES keys to produce an effective key length of 168 bits. Triple DES was created because of the DES algorithm, invented in the early 1970s using a 56-bit key. The effective security Triple DES provides is only 112 bits due to meet-in-the-middle attacks. Triple DES runs three times slower than DES, but is much more secure if used properly. The procedure for encrypting something is the same as the procedure for encryption, except it is executed in reverse. In DES, data is encrypted and decrypted in 64 -bit chunks. The input key for DES is 64 bits long; the actual key used by DES is only 56 bits in length.The least significant (right-most) bit in each byte is a parity bit, and should be set so that there are always an odd number of 1s in every byte. These parity bits are ignored, so only the seven most significant bits of each byte are used, resulting in a key length of 56 bits. This means that the effective key strength for Triple DES is actually 168 bits because each of the three keys contains 8 parity bits that are not used during the encryption process.DES is a type of computerized cryptography where block cipher algorithms are applied three times to each data block. The key size is increased in Triple DES to ensure additional security through encryption capabilities. Each Block contains 64 bits of data. Three keys are referred to as bundle keys with 56 bits per key. There are three key options in data encryption standards:

A. All keys being independent

B. Key 1 and key 2 being independent keys.

C. All keys are identical.

Although, option C is discarded because it is least secure.

Triple DES algorithm uses three iterations of common DES cipher. It receives a secret 168-bit key, which is divided into three 56-bit keys.

•Encryption using the first secret key

•Decryption using the second secret key

•Encryption using the third secret key

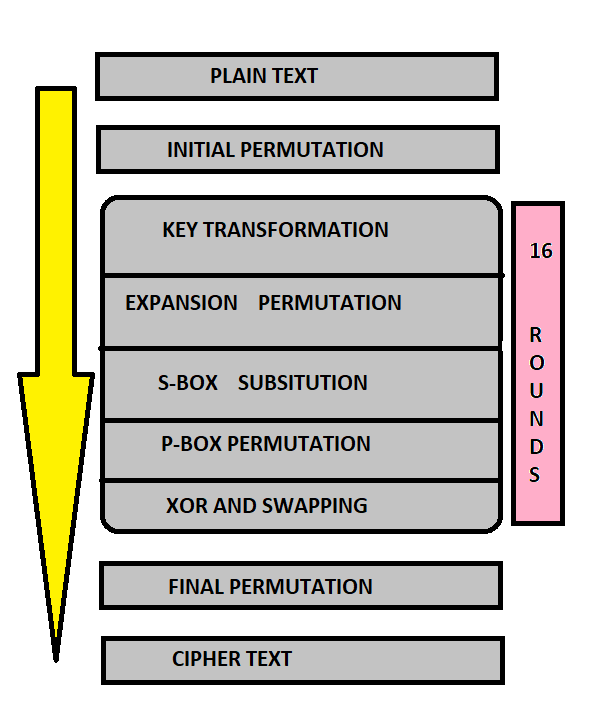
Encryption: c = E3 (D2 (E1 (m)))

Decryption: m = D1 (E2 (D3(c))) Using decryption in the second step during encryption provides backward compatibility with the common DES Algorithm. In these cases, the first and second secret keys or second and third secret keys are the same whichever key.

c = E3 (D1 (E1 (m))) = E3 (m)c = E3 (D3 (E1 (m))) = E1 (m).

It is possible to use a Triple DES cipher with a secret 112-bit key. In this case first and third secret keys are the same.

c = E1 (D2 (E1 (m)))



**FIGURE 5: WORKING OF DES ALGORITHM**

**Wavelet Based Triple DES**: In this paper, a new image encryption algorithm is proposed. First of all, wavelet decomposition is used for concentrating original image in low-frequency wavelet coefficients, then the DES algorithm is applied to encrypt the low-frequency wavelet coefficients. Secondly, an XOR operation is used for high-frequency wavelet coefficients and the encrypted low-frequency wavelet coefficients (as a key stream), so that the image information contained in high-frequency wavelet coefficients is hidden; thirdly, a wavelet reconstruction is used for spreading the encrypted low-frequency part to the whole image. Let’s call the output as **WAVELET OUTPUT**.

Now, in our method, we are modifying the key constraints. Since, most popular key constraints are

1. All keys are independent.  
   A. Key K1 : user’s fingerprint  
   B. Key K2 : ATM Card Number  
   C. Key K3 : 4-Digit PIN
2. K1,K2 are independent. <ENCRYPT ,DECRYPT ,ENCRYPT>  
   A. Key K1,K3: user’s fingerprint  
   B. Key K2: 4-Digit Pin

The binary data that was obtained from the image of digital signature is fed to the processor encrypting the data with the help of the **user’s fingerprint** as an **encrypted key**. The data is encrypted using wavelet based Triple DES technology as suggested above to get the **WAVELET OUTPUT** and **accordingly Keys K2 and K3 are further used to encrypt depending on which type of key constraints are adopted in ATM MACHINES** and then the final encrypted image is passed on to the bank server through a communication link. At the bank side, the received cipher message is decrypted with the help of the same key( as the fingerprint is stored in the bank's database along with the PIN and ATM Card Number). The original image is reproduced at this step. Then the decrypted image of digital signature is matched with the previously stored image of the authentic customer for the specific request of the client. If the request is valid then an acknowledgement message is sent to the ATM machine through the same communication link. If the acknowledgement is “Yes” , the client can withdraw money from the ATM machine. If acknowledgement is “No” an error message is shown on the screen of the ATM machine.

**Special Cases:**

**Case 1:** For those who are less educated or don’t know how to write, while registering their signature at the bank, they are expected to just draw simple patterns like triangle, star etc. Since, what is important is their style of handwriting. This ensures that no one is left out.

**Case 2:** If someone forgets their signature as in the case many people have different signatures for different bank accounts. For them, they will tap on the **FORGOT SIGNATURE?** option and then they will be prompted to tap on the pad their mobile number.  (**NOTE: The signature pad has also 0 to 9 numbers on one corner**). A One Time Password [OTP] will be sent to the phone number. Note that since the user is tapping on the numbers using a digital pen, his fingerprint is already recorded and since fingerprint is associated with the card number and card number is mapped to mobile number thus, verification takes place simultaneously. The user taps the OTP thus received, on the pad and if the OTP is correct access is granted and the user can make the transaction. A time-limit will be set and 3 such attempts can be made then the account gets locked.

**Case 3:** If it is a third-party user (for instance, father asked his son to go to the ATM and withdraw money on his behalf), the scenario would be like ->the user will tap on the option of **THIRD-PARTY USER**, then the user will enter his/her mobile number. A toll-free call will be made to the genuine user on behalf of whom the third-party user has come to withdraw money. The toll-free call is made possible because the ATM card is linked with the mobile number of the genuine user. The call will be made to the genuine person because the third-party user has inserted the ATM debit card of the genuine user. The genuine user picks up the call on which he would be asked to press 1 for allowing the third-party user to allow access else press 2 for denial. Accordingly, the third- party user gets the access or denial. Note: It is really hard to breach into secure transactions when the genuine user goes to the ATM. So, in order to cover up the loop-hole as it could have been in case of Third-Party Option we have preferred security over user’s comfort.

The following points are to be noted:

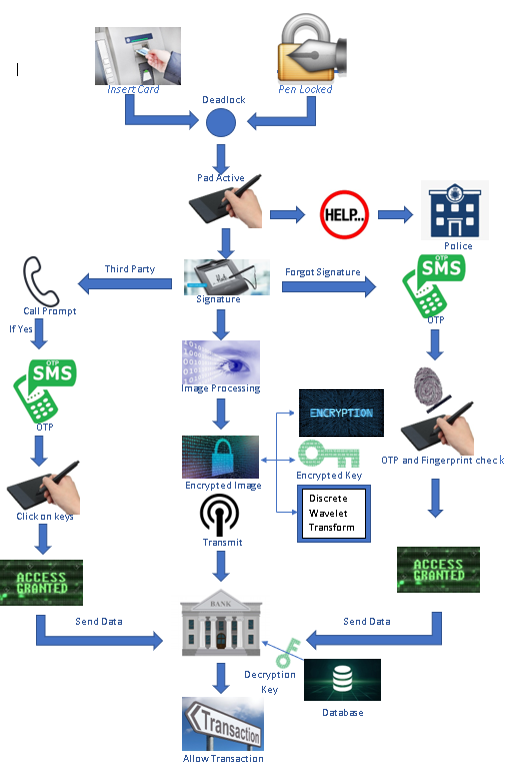
* **Solution Type (Hardware/ Software):** Both Hardware and Software.
* **Solution Capabilities :**   
     1. **Preventive**: It prevents hacking the data in transmission media since WAVELET   BASED Triple DES IS USED.

   2. **Detective:** It detects if a user is malicious for example in case of third-party.

   3. **Responsive:** informs the police station etc. in case of any threat caused by a  forcing criminal and also prompts the genuine user if an illegal third party user is trying to  access the account and accordingly the genuine user can respond to it.

* **Scalability**: Installing the hardware like digital pen and pad is a one-time investment and rest of the security is ensured after installation.(as we have managed security against theft activities like pen stealing as explained earlier.) So once installed, it is highly scalable.
* **Platform Dependence:** Yes, it is dependent on the hardware.
* **Deployment Model:** Premises i.e. installation in ATM booths.
* **Performance:** The proposed system is one of the most secured and least energy consumed systems compared to the existing ATM systems. There are two reasons;first, the acquisition device captures the image accurately. The error of the device is negligible. Secondly, using Triple DES makes the system more secure, fast and energy efficient.

**Process Flow Diagram:**

****

**6. How would you estimate the Risk Mitigated/ Reduced by deploying your solution? (You may explain using Qualitative and/or Quantitative Approach) \***

* **The 4 Digit PIN** is easy to crack using dictionary attack, thermal foot-printing and many more. The 4 Digit pin can be traced easily and therefore not secure in this modern era. The fingerprint pattern based upon our ridges and valleys of our fingers and different minutiae patterns, gives uniqueness as no two persons have the same fingerprint. On the other hand, our digital signature gets its uniqueness because people have different styles of writing, different signatures, different writing times and different ways of holding the pen. All of these parameters are recorded and it becomes very difficult to imitate all of the attributes simultaneously.
* **Fake ATMs:** When an ATM is installed, it has to be configured with a digital pen i.e. for an authentic ATM there should be a token (set by the bank) to configure with the digital pen. That means even if someone installs a fake ATM it would not be configured with the pen since the token is given by the bank only to authentic ATMs.
* **Shoulder Surfing:** Considering the worst case that signature is recorded including the way of writing, pen movement angle and other parameters, still the attacker cannot get the access since after all, both signature and genuine user’s fingerprints are needed to unlock the 2-way lock. Moreover, it is rarely possible to copy the exact parameters of handwriting as that in case of a genuine user.
* **Fake keypad-overlay attack:** Since the digital pen will work only with its signature pad pair, this attack cannot occur. The pair is configured with an authentic token for pen and pad set by the bank.
* **Criminal Forcing:** Since, the criminal waiting outside the booth for the user to withdraw the money and give it to him, the user inside just has to write HELP or मदद and then just like the emergency call services in a mobile phone, an alert message will go to the control room of the bank as well as to the nearby police station. The information sent to the control room will include the ATM Booth Location and Card Number so that necessary action takes place. The CCTV camera installed in every ATM booth records the face of the innocent and further investigation measures can be taken.
* **Skimming:** This problem is overcome using our One Time Password [OTP] scheme which is explained in the procedure and Process Flow Diagram.
* **Theft Of Digital Pen:** The pen is held by a holder which also serves as the lock. Without inserting the ATM Card, the lock will not open.Any attempt to forcefully take out the pen will trigger the alarm. Since, the pen is linked with the pad using a token it has a set distance radius such that if the pen is beyond that radius alarm will be triggered. So, even if someone inserts the ATM card and tries to steal the pen away , his plan would fail.
* **Triple DES:** Since Triple DES is not very secure, our approach in modifying the algorithm ensures incredibly high safety and attacks like brute-forcing and meet-in-the-middle would not work because fingerprints and digital signature are shared with nobody and is really difficult to copy.

**7. Explain business use case of your innovation (with Examples)\***

The main use case is stealing of pen which can be prevented by deadlock technique until the  card is fully inserted into the card holder of atm the pen cannot be unlocked and when the pen unlocked pad become active only for a particular pen linked with a token and no duplicate pen can be used  client can use to sign on pad. If the signature is authenticated a message from the bank came which means a yes . Then the transaction can be done afterwards. After a successful transaction the user has to keep the pen in the holder in order to free up its card. After the pen is kept in the holder, the pen is locked and the card is released. Since, the pen is linked with the pad using a token it has a set distance radius such that if the pen is beyond that radius alarm will be triggered. So, even if someone inserts the ATM card and tries to steal the pen away, his plan would fail.

**8. What is the USP of your innovation? (For EG. Time Saved, Improved Efficiency Etc.)** \*

Our Product is the first ever product of its kind which enforces two biometric attributes (fingerprint and digital signature where digital signature is a behavioral attribute) and provides highly secured encryption of biometric information by modifying Triple DES Algorithm and encrypting the ultra-sensitive information in no time. The algorithm ensures data integrity.

Thus, our product is highly efficient and secured.

Obviously, any company wants to ensure its customer’s safety and when the customers feel safe, they will be interested in using the product which leads to higher demand for the product. Our product proudly accomplishes this task.

**Solution Technical Feasibility**

As the debit cards have expiry dates of 2-3 years they have to renew it in this span so when they come to banks we change their cards to the new ones and help them understand the usage of new technology and save their required credentials in the database. It is fast and secure as compared to conventional means.Though, we provide many facilities taken in mind the needs of customers.

**9. Does your innovation require assistance from existing products?\***

Yes, for hardware, we require CMOS based Fingerprint Sensor and Digital Pen-Signature Pad kit.

For software, we require the Triple DES encryption standard and database of banks for storing information of ATM Card holders.

**10. Does your innovation have relevance to an existing or emerging technical standard? (A technical standard is a set of requirements for ensuring interoperability among devices or promoting reliability, productivity, efficiency, or safety of devices)\***

Yes, CMOS Based Fingerprint Sensor is used for common mode noise reduction as well as taking care of wet and dry fingers by making use of differential integrators and two-phase mode.[6].

We are also modifying the existing Triple DES standard to Wavelet Based Triple DES Standard [1].

**11. Briefly describe key technical hurdles that need to be overcome to implement your innovation, and the resources required to do so.\***

* Installment of signature pad-digital pen kit on each ATM and configuring each ATM with digital pen kit and removal of number pad from the ATMs.
* Storing digital signature and fingerprint for each debit card user in the bank’s database.

**12. Are there any key partners whom you plan to work with to develop the technology?\***

* **Semiconductor industry:** We would require a semiconductor industry to coat our digital pen with CMOS-Based Capacitive Sensors.
* Eventually after our model is implemented then we will be working with research graduates who will be helping us to increase the security level of our model to improve our product and will be able to provide the best services to the user.

**13. What difference will the funding make on the solution (such as faster to market, more partners and reduced risk\***

Funding makes our solution more reliable and helps to implement it faster because debit cards expire every two to three years and everyone has to renew it so by manufacturing our product as soon as possible upto the current demand we can change the existing technology easily and more conveniently.

**Roadmap**

**14. What is the planned roadmap for the company in the short and long term? (Share details about expansion plans, plans for ramping up production/development, collaborations/tie-ups being sought, garner support from relevant bodies/regulators) \***

* We have planned to help the government in order to increase the ranking of India in terms of technology aspects as well as standards of living. No doubt, this is the first step towards our motto.
* For the short term we have to implement this as soon as possible and most preferably satisfy customer demands not only technically but also in terms of their convenience. Moreover, we will be finding like-minds who can help us to make our product better and more reliable. We will be establishing a publicity team which will look after attracting the people and will help to promote our product.
* Keeping in mind our country’s economy, we did not switch Triple DES technology to AES (Advanced Encryption Standard) because it is highly expensive and implementing AES and replacing the processor with the AES Processor is both time consuming and costly. As trained engineers, we focus on developing technologies which saves time and money. Modifying the Triple DES standard and making use of biometrics, we have not only solved most of the security breaches against ATM machines but also have saved money.

For the long term:-

* We will establish a R&D(Research and Development) team which regularly looks at the bright and dark side of the product.
* We will be establishing a sales team which will look after the sales.
* We will look to attract more and more investors which will increase our economic value in the market.
* We will try to expand our product globally so as to provide the best services in the world.
* Modification in The Triple DES Standard would flourish throughout the world as the entire globe is thinking to improve the transaction processes. This need would increase the popularity of our country since our country came up with this idea. This way, we are able to keep up our motto.

**MARKET**

**15. What is your Addressable Market & Growth Potential of the market & which companies or investors are most likely to be interested in this invention? (Explain keeping the following points in mind: Does your idea have a natural sales appeal? Is the market ready for it? What evidence is there that the market will be willing to buy your solution? Can customers afford it? Will they buy it? Is there a timing factor?)\***

**Addressable Market:-1. What do they look like?**

* **Demographics** — In our model we will be focusing on both B2B (Business to Business) and B2C(Business to Customer) services. B2B are the banking industry whether private and government banks .On the other hand B2C are the common people availing the bank facilities and have atm cards.
* **Psychographics** — The consumers who have the knowledge on how to use ATM cards and are literate as per Indian survey standards.

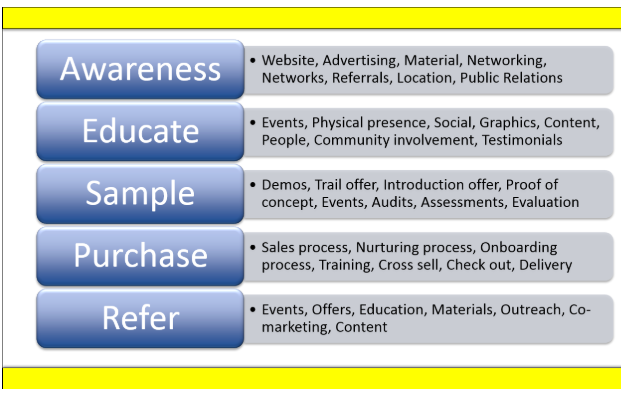
**Challenges or Problems** — Today’s atm machine transactions are less secure and atm transaction details are easily hacked by a well known hacker. ATM fraud increases  over time, depending on what crimes are targeting the machines. More than half of executives surveyed state ATM losses are up in 2016 compared with 2015; 32 percent state they are up between 1 percent and 9.9 percent, while 23 percent state they are up 10 percent or more.

**2. What are their problems?**

Since we are providing a new model to protect the consumers from frauds, criminals and hackers who manage to infiltrate the communication media and steal sensitive banking information. Thus, using our model will make the transaction more secure.

**3. How do they want to be served?**

Today we are living in 21 st century and we are evolving across technology. Daily we get to know about new technologies.It is correctly said that “Value is in eyes of the beholder”, Today’s life is too near to gadgets that we are finding a way to make things easy. Today’s customers want everything secured ,convenient and want to be served to the best.



**Growth Potential Market :-**



**Market size –** A per The Hindu newspaper  published on  Jan 6th, 2018 Total   no. of ATMs in India : 2.04 lakh (approx) Out of which 1.10 lakh are in the National Capital Region . They belong to different private and government banks.

**Market growth –** As India is a developing country and is moving towards technology and secure gadgets Thus our model has a  great chance to grow in the market and attract many investors and banks to use our new technology.

**Profitability –** We will get profit from manufacturing kits to be installed in the atm and the modified softwares which we will be providing to the customers. The hardware is a one time installment process and the software we are providing only requires maintenance cost and banks server maintenance cost  which is periodically . Hence these expenses will be providing benefits to both our customers using our technology .

**Competition** –There are very few companies which provide security facilities to the banks . Thus we will get very less competition in the market and help our company to grow exponentially and will help to make our company earn profit.

**Companies or investors :-** any company requiring a secure payment system, for example paytm, other banks, TAC security(indian company)

Investment from any company looking to enter the market, or penetrate the current “king”

**16. How will you determine whether your target market likes your solution, or your concept?\***

The factors which we are using to determine whether your target market likes our solution or our concept

**1.Fraud Rate:** We will be focussing on the measurement of fraud rate and we will look at how fraud rate is decreasing in the country periodically.

**2.Profit:** We will be looking at how our profit is increasing and will be looking at how to increase our production regularly.

**3.Security:** We will conduct regular polls on social media and on our website to get regular feedback from banks and consumers who will be using our products and hold seminars such as feedback sessions in the bank to know how our product helps the bank employees and customers.

**4.Semiconductor market:** We will be regularly contacting the semiconductor market which manufactures the hardware we use and take updates to increase the reliability of the hardware.

**5.Media involvement:** Since we are developing a product for banking industries governed by RBI (Reserve Bank of India) ,the media will play an important role to tell us how we can improve our product and provide better services.

**6.** Obviously, any company wants to ensure its customer’s safety and when the customers feel safe, they will be interested in using the product which leads to higher demand for the product. Our product proudly accomplishes this task.

**17. How will you estimate the Return on Investment (ROI) of your solution?\***

Current market has banks with an investment of 1 million on ATM's in India,and also 2,50,000 on the research or other secure solutions to keep them safe, that's where we step in, instead of spending that amount on other solutions that are less efficient, spend some of that amount on our model which can be seen in our cost.

We will be having a legal contract with the banks under which they have to pay for our manufactured kit and periodically for our updates whenever the product is being updated .

**18. How is your solution more appealing than existing products in the market (if any)? (In design, quality or additional features)\***

* Our product is way more secure than the existing technologies used in ATMs at both hardware and software level. When it comes to money, everyone wants to keep it safe especially when we are making transactions digitally. Securing information biometrically will keep their information safe. So, our model will definitely be eye-catching !
* Moreover, with the rise in the recognition of **DIGITAL INDIA CAMPAIGN** , people would gladly participate in making our country more secure and digitally advanced.
* Our direct customers i.e. both private and public banks are aware of the people feeling safe about transactions, so more people would step in on opening their bank accounts and issuing debit cards, so banks would gladly adopt our idea.

**19. Succinctly state why your company should win this award. (Please provide any additional information/supporting documents /testimonials that hasn't been covered in the above questionnaire, but that you feel will underpin your nomination)\***

* Since, we are using the most advanced technologies to make our one-time investment product yet at low power consumption and on a real time basis which enhances its efficiency and makes our model error free. We guarantee that our product would not let anyone down on the basis of security breaches and it is just the needed product that our country demands from an era where technology makes the revolution.
* Keeping in mind our country’s economy, we did not switch Triple DES technology to AES (Advanced Encryption Standard) because it is highly expensive and implementing AES and replacing the processor with the AES Processor is both time consuming and costly. As trained engineers, we focus on developing technologies which saves time and money. Modifying the Triple DES standard and making use of biometrics, we have not only solved most of the security breaches against ATM machines but also have saved money.
* If our product is recognized by the government, it would sky-rocket our idea of making our country digitally safe and protected. Not to mention, our sales would be sky-rocketed too.

**20. Briefly explain the following:\***

**Sales Distribution Channel**

* **Direct**:-Since our product will be for both private and public banks thus, we will initially be reaching in the banking industry ourselves to promote our product and as we expand our business we will be including the sales team which will be selling our product.
* **Value-Added Reseller (VAR):-**Initially, we are not looking for any reseller to buy our product to sell it on e-commerce or any other platform.
* **Consultant:-**We consulted our teaching mentor for the sales distribution channel.

Go to Market Strategy, Time to Market

**1. What is your business case?**

We are launching this product right to increase the security level of ATMs as soon as possible. Going to the well-established market is tough “But change is the law of nature” and we want high end security .The given case will help to increase our sales and will help us to expand our market exponentially

**2. Define your market strategy.**

* **Value props**: We integrate with more tools than have already been used and our product is more secure than any other.
* **Messaging:**

**1.**  We will be telling the customers about how safe their ATM cards become after using our technology.

**2**. Will tell the banking industry how our product makes banking transactions easier and more encrypted.

**3.** Will Show how our model helps to promote digital banking and safe transactions via communication media.

* **Sales and support materials:** We do have research papers as supporting material to show how our model is better than the one which we use.
* **Customer journey:** The customer when ready to buy our product will first have to sign legal documents which will assure that we have a legal contract and then will be selling our product to him keeping our algorithms as confidential.
* **Personas**: Banking industry is our main business partner and indirectly will be focusing on customers using the banking facilities.

**3. Lock in your pricing strategy:-**

Pricing is more than just a financial decision. It would cost around 20,000-30,000 INR.

**4. Create your external marketing plan**

* Branding: The brand partners which the banks are using will help us to promote our product.
* Content is a powerful way to get in front of potential customers and show them that you’re knowledgeable and trustworthy. Our content strategy can help support your launch with things like blog posts, videos, ebooks, and whitepapers.
* Events, ads, and PR: When we establish a well known market then will be looking for events,ads and pr.

Cost of developing the product:

* Digital Pen and Signature Pad: INR 15,000-20000
* CMOS-Capacitive Sensors:- INR 5,000- 10,000
* Buzzer Alarm: INR 500-1000
* Pen Holder with Charging facility: INR 300

**References:**

1. [**Enhanced ATM Security using Biometric Authentication and Wavelet Based AES**](https://www.matec-conferences.org/articles/matecconf/pdf/2016/05/matecconf_iccma2016_06003.pdf)
2. [**Secure Communication Protocol for ATM Using TLS Handshake**](https://pdfs.semanticscholar.org/457e/6d60bb5f90ab0037f959886a4fd24eef1fb6.pdf)
3. [**(PDF) A Reliable ATM Protocol and Comparative Analysis on Various Parameters with Other ATM Protocols**](https://www.researchgate.net/publication/273260669_A_Reliable_ATM_Protocol_and_Comparative_Analysis_on_Various_Parameters_with_Other_ATM_Protocols)
4. [**https://shodhganga.inflibnet.ac.in/bitstream/10603/25038/9/chapter-5.pdf**](https://shodhganga.inflibnet.ac.in/bitstream/10603/25038/9/chapter-5.pdf)
5. [**Japanese bank introducing biometric ATMs to open accounts**](https://www.biometricupdate.com/201901/japanese-bank-introducing-biometric-atms-to-open-accounts)
6. [**CMOS Capacitive Fingerprint Sensor Based on Differential Sensing Circuit with Noise Cancellation**](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6069013/)
7. [**Online handwritten signature verification system based on DWT features extraction and neural network classification**](https://www.sciencedirect.com/science/article/pii/S2090447910000080)