***LITERATURE SURVEY:***

What is Single-factor Authentication (SFA):

Single-factor authentication is the simplest form of authentication methods. With SFA, a person matches one credential to verify himself or herself online. The most popular example of this would be a password (credential) to a username. Most verification today uses this type of authentication method.

## What is Two-factor Authentication (2FA):

Two-factor authentication uses the same password/username combination, but with the addition of being asked to verify who a person is by using something only he or she owns, such as a mobile device. Putting it simply: it uses two factors to confirm an identity.

## What is Multi-factor Authentication (MFA):

## Multi-factor Authentication uses a combination of the following factors: something you know, something you have and something you are. 2FA is a subset of MFA.

In recent years, the development in Information technology has unleashed new challenges and opportunities for new authentication systems and protocols. Authentication ensures that a user is who they claim to be. The trust of authenticity increases exponentially when more factors are involved in the verification process. When security infrastructure makes use of two or more distinct and different category of authentication mechanisms to increase the protection for valid authentication, It is referred to as Strong Authentication or Multifactor Authentication. Multifactor authentication uses combinations of "Something you know," "Something you have,", "Something you are" and “Somewhere you are”, “Someone you know”, to provide stronger remote authentication than traditional, unreliable single-factor username and password authentication. In this paper we do a survey on the different aspects of multifactor authentication, its need, its techniques and its impact.

Multi-factor authentication methods are difficult to compromise than single-factor methods. Let us take for example, the use of a logon ID/password is single-factor authentication (i.e., something the user knows); whereas, an ATM transaction requires multifactor authentication: something the user possesses (i.e., the card) combined with something the user knows (i.e., PIN). “Out-of-band” controls for risk mitigation can also be included in multifactor authentication methodology. An effective authentication method should have customer acceptance, reliable performance, scalability to accommodate growth, and interoperability with existing systems and future plans

**Online Banking Fraud:**

**Internet** **Banking** **Fraud** is a **fraud** or theft committed using **online** technology to illegally remove money from a **bank** account and/or transfer money to an account in a different bank. **Online** **bank** **fraud** is one of the most widespread forms of cybercrime.

There are mainly 2 Types of Online Frauds:

**User Identity Theft:**

Identity theft is the **deliberate use of someone else's identity**, usually as a method to gain a financial advantage or obtain credit and other benefits in the other person's name, and perhaps to the other person's disadvantage or loss.

**User Session Hijacking:**

Session hijacking occurs **when a session token is sent to a client browser from the Web server following the successful authentication of a client logon**. A session hijacking attack works when it compromises the token by either confiscating or guessing what an authentic token session will be, thus acquiring unauthorized access to the Web server.

**FFIEC guidelines provide four specific measures for consideration:**

* Identify and assess threats to consumer information by performing a risk assessment
* Create a plan, in writing, with policies and procedures to minimize risks
* Implement and test the plan
* Adjust the plan as technology changes, as customer data changes, and to address shifting threats (internal or external)

**->**

According to the Mobile Payment Forum, mobile payments are the transactions with a monetary value that is conducted through a mobile telecommunications network through diverse mobile users devices, such as cellular telephones, smart phones or PDAs, and mobile terminals. Mobile payment is a transfer of funds in return for goods or services in which a mobile device is functionally involved in executing and confirming payment. The payer can be standing at a POS or be interacting with a merchant located somewhere else. Mobile payment systems enable customers to purchase and pay for goods or services via mobile phones. Here, each mobile phone is used as the personal payment tool in connection with the remote sales. Payments can take place far away from both the recipient and the bank

**TRANSACTION FLOW OF THE PROTOCOL**

As days are passing online payments is getting popular and for this people uses various modes of payment like Debit card, Credit Card, electronic wallet, e-banking etc. People purchase products over the internet and also pay the bill online, which is easy to implement and also saves the time. But the only question that comes in the mind of every person is about the security of data which has been shared by the person while online payment

When it comes to the communication of sensitive data security has always been an important topic. With hardware advances allowing users the advantage of accessibility used in mobile devices, individuals are now spending more and more time on these devices. Additionally, with the viral popularity of social media applications and single sign-on, users do not always take as many precautions as needed with their information. Multi-factor authentication creates more and varied walls to block out the wrong people from seeing your information

Basically now-a-days mobiles comprises of the basic authentication required which can be treated as the first factor authentication and the other two factors need to be implemented as follows,

The process of authentication is essential for allowing users to enter credentials and if they matches with the existing one then user is authenticated user and is allowed to login to the system otherwise not. This is the initial factor authentication which also gives control access to system by verifying each user and giving access to only verified ones. Now Addition of other factor authentication is a security mechanism which uses two of the three factors of credentials for authentication. The two-factor authentication works with two separate security mechanisms. Typically one is a physical validation token, and one is a logical code or password. Both must be validated before accessing a secured service or product. Now coming to the multiple factor authentication is a mobile authentication/ financial transaction System using a unique mobile identification code and method thereof, where in mobile authentication and/or financial transaction are carried out without replacing a mobile communication terminal in Such a way that various authentication and/or financial transaction are performed based on the unique mobile identification code received from a mobile communication terminal according to a Standardized mobile communication protocol

And the flow of implementation will be as follows, The merchant will first register a source of funds and a payer device with a unique ID with the payment server. Then once a merchant and the payer have agreed on a financial transaction amount, the merchant requests a transaction ID from the payment server for that amount. The payment server sends the merchant a transaction ID, which the merchant then communicates to the payer. The payer in turn relays this transaction ID to the server, which validates the transaction using the payer device. The server then releases funds to the merchant. The server can preserve all records for auditing purposes, but security is enhanced because the merchant never gets direct access to the customer's financial account information

Therefore we consider 4 phases in the transaction flow of the system as follows,

1. Firstly, the basic login i.e validating the credentials of user/payer

2. Performing of Two factor authentication

3. Now validating of the Transaction Identification Code (TIC).

4. SMS Confirmation.

In an alternative approach that is used by some mobile payment services providers, for example Ericsson IPX, to purchase online goods, the payer (i.e. customer) provides a mobile phone number to merchant, which then presents the phone number to the Ericcson payment system. The payment system in-turn provides the payer with a short passcode number (PIN). The payer gives this PIN to the merchant. Upon receiving this PIN, the merchant then releases the on-line goods. The payment funds ultimately come from the payer's mobile phone bill.

The drawback of this approach is payer needs to share his personal information, for example phone number with the merchant site. Separately this process is bit inconvenient for the payer since he has to first enter information on the payee site and then read PIN from his cell phone, and then enter PIN into merchant’s online site

An alternate method of payment that utilizes a temporary and usually a one-time use transaction “identifier” or code (transaction ID). This transaction ID does allow a payment to be tied to a customer's (payers) financial information, but does not require that the payer's sensitive financial information be transmitted to a potentially insecure merchant (payee) or other provider of goods and services .The invention is further based, in part, on the idea that this transaction ID should preferably be short enough to be easily communicated by humans (e.g. a 10 character or less code, rather than a large 30+ character code). As previously discussed this transaction ID should often be good for only a single transaction, and/or be valid for only a relatively limited period of time. Such as a week, day, hour, or even minute. Here the shorter the period of time in which the transaction ID is valid, the fewer the number of unique transactions that be supported by this particular transaction ID. This can result in improved convenience for the payer, but of course overly short time periods can also result in inconvenience and an occasional need to repeat valid transactions. This short period can be adjusted to achieve a good trade-off between security and convenience.

Encryption algorithm plays very important role in communication security, On a survey the performance of existing encryption techniques like AES, DES and RSA algorithms is as follows ,Based on the text files used and the experimental result it was concluded that AES algorithm consumes least encryption and RSA consume longest encryption time . From the simulation result, we evaluated that AES algorithm is much better than DES and RSA algorithm.

**SECURITY AGAINST PHISHING**

**Phishing** is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

**Phishing(prevention):**

To prevent from phishing **attack**, you should never share your personal or financially sensitive information such as login credentials or credit card details as over the Internet. Most of the phishing emails will re-direct you to pages where the entries for financial or personal information are required.

**Virus Attack on Cell Phones &PDAs:**

Most current cell phones have the ability tosend and receive text messages. Some cell phones and PDAs also offer the ability to connect to the Internet. Although these are features that you might find useful and convenient, attackers may try to take advantage of them.

* abuse your service.
* lure you to a malicious web site.
* use your cell phone or PDA in an attack.
* gain access to account information.

**Virus Attack on Cell Phones & PDAs(prevention):**

* Apply available critical patches and upgrades to the operating system
* ­ Eliminate or disable unnecessary services and applications
* ­ Install and configure additional applications that are needed
* ­ Configure user authentication and access controls
* ­ Configure resource controls
* ­ Install and configure additional security controls that are required, including content encryption, remote content erasure, firewall, antivirus, intrusion detection, antispam, and virtual private network (VPN) software ­
* Perform security testing.

**User Session Hijacking:**

Session Hijacking is an attack which is basically used to gain the unauthorized access between an authorized session connections. This is usually done to attack the social network website and banking websites in order to gain the access over the valid session as well as over the website too. These attacks are one of the commonly experienced cyber threats in today’s network. Most of the websites and networks are vulnerable from this kind of attack. For providing the protection I have given the multiple ways to protecting from this session hijacking attack. I have especially focused on one of the major attacks in this session hijacking attack SSL Strip attack which play very vital role in this kind of attack. Sometimes this session hijacking attack is also known as the Man in the Middle attack (MIMA).In this paper, I have covered many security mechanisms to stay away and protect you and the network. This session hijacking attack is very dangers for the security perspective. Even it can steal all users’ most sensitive data.

**TECHNOLOGIES**

**J2ME:**

With mobile commerce technology continuously being taken more into use and introduced in new markets, the transition to mobile commerce (m-commerce) will make mobile shopping exceedingly popular.In the near future mobile shopping will probably replace today's markets or shopping complex. This project presents a mobile application which is built using Mobile Information Device Profile (MIDP) of the Java 2 Platform Micro Edition (J2ME), that enable users to purchase flowers without a trip to the market or elsewhere.

**J2ME Toolkit Features:**

* Support for obfuscation in the build cycle.
* Method profiling.
* Memory monitoring.
* Network monitoring.
* Device speed emulation.

**JDK:**

The **JDK** is a key platform component for building **Java** applications. At its heart is the **Java** compiler. The **Java** Development Kit (**JDK**) is one of three core technology packages used in **Java** programming, along with the JVM (**Java** Virtual Machine) and the JRE (**Java** Runtime Environment).

**JDK Security Features types:**

* Users running programs.
* Developers
* Systems administrators, developers, and users.

**Java Servlet:**

A **servlet** is a **Java programming** language class that is used to extend the capabilities of servers that host applications accessed by **means** of a request-response **programming** model. Although **servlets** can respond to any type of request, they are commonly used to extend the applications hosted by web servers.

**JDBC:**

The Java Database Connectivity (JDBC) specification is a new basis for developers to interface with data sources. The structure of the JDBC is designed to allow developers to program for a standard interface, and let the low-level JDBC driver for different databases deal with the connection and querying of the databases; hence, the developer does not need to worry about dealing with different SQL flavors for each database. The JDBC is also very flexible. A developer doesn’t necessarily lose features specific to the target database. Best of all, the JDBC is based on the Java language!

**ORACLE 9i with JServer:**

Oracle9i Application Server provides the lowest total cost of ownership of any application server on the market, by delivering the most comprehensive, standards-based functionality from a single fully integrated e-Business platform.

**Authentication of the user to the Bank authentication Server based on user login/password**

**What user authentication is**

User authentication is a security process that covers all of the human-to-computer interactions that require the user to register and log in. Said more simply, authentication asks each user, “who are you?” and verifies their response.

**To put it simply, user authentication has three tasks**:

* Manage the connection between the human (user) and the website’s server (computer).
* Verify users’ identities.
* Approve (or decline) the authentication so the system can move to authorizing the user.

### Password-Based User Authentication Methods

Most users are familiar with passwords. In fact, passwords have been the tried-and-true method for user authentication since the beginning of the internet. You probably have quite a few passwords yourself!

**A password-based user authentication process generally looks like this:**

* When you land on the page, you’ll be asked to enter your username and password.
* Your credentials are sent to the website’s server and compared with the information they have on file.
* When a match is found, you’ll be able to enter your account.

Passwords are often used to secure personal accounts like social media profiles, online banking and eCommerce sites, and other online resources. However, passwords are not as secure an option as many users think they are. And a lot of damage can be done if a hacker is able to gain access to one of these accounts!

To top it all off, [users are managing an average of 90 accounts](https://digitalguardian.com/blog/uncovering-password-habits-are-users-password-security-habits-improving-infographic#:~:text=In%20fact%2C%20a%20Dashlane%20analysis,to%20a%20single%20email%20address.)—and that’s just in our personal lives.

That’s a lot of passwords to keep track of! As a result, many users have chosen convenience over security. Instead of creating strong passwords, most users use a simple arrangement of letters, numbers, and symbols because it’s easier to remember.

**Authentication of the user to the Bank or Financial Institution authentication server based on TIC verification**

**TIC GENERATION AND DISTRIBUTION:**

Important module in the protocol is generation of TIC codes at the financial institution server, distribution of TIC’s to the customer and encryption of TIC’s before storing them on client environment. TIC codes are pseudo random codes and can be generated with pseudo random number generation algorithm.

**TIC AUTHENTICATION:**

TIC Authentication is the technique which is used to identify both the user and the ongoing transaction. TIC code certifies that the current transaction has been initiated by the right person and it is a valid user who is trying to access account. TIC code is:

* Issued by the Bank or Financial institution to its customer.
* 8 bit or 16 bit Pseudo randomly generated code which is assigned to the customers.
* May be complicated digit sequence or combination of numeric or alpha numeric characters.
* One TIC code is used only once that is a unique TIC is used for each transaction.

It is assumed that financial institutions are responsible to store TIC generation logic and algorithm confidentially and have specific parameters to decide the complexity of TICs format. Financial institutions are also responsible for upgrading from time to time the TIC generation logic and data and also to keep it absolutely secret. The user will get the list of TIC codes from the bank or financial institution according to its requirement.

Financial institution will keep the record of issued TIC codes to its customers and match the same code during the online web transaction. A TIC code is cancelled after each successful transaction. Validity time period of TICs can be decided according to issuing organization policies, which provides an extra security feature in the system.

**Authentication of the user to the Bank authentication server by SMS confirmation.**

**SMS AUTHENTICATION:**

Another method to validate user transaction is an SMS confirmation. Financial institution stores user cell phone number to provide multifactor authentication. It is believed that users will carry cell phone and can receive/send the short message. As a result, only valid users who have account will receive confirmation SMS from the authentication server. After getting an SMS the user can acknowledge the choices. When authentication server receives ―YES‖ than it is taken that the user is valid and the user may be allowed to initiate the transaction. On other hand, if the user sends a ―No‖ or the user does notsend any response within a specified time period then the transaction will be rolled back and terminated.

**SMS CONFIRMATION:**

After the TIC code identification and validation the remainder of the transaction will proceed. At the end of the transaction the user will get an SMS from the web authentication server to confirm financial transaction. Security of the proposed system will also depend on the security of encrypted messages sent by SMS and algorithm used for message encryption.