Chapter – 6

STEPS TO IMPROVE

E-SECURITY

AND MITIGATE

E-FRAUDS
Chapter – 6

STEPS TO IMPROVE E-SECURITY
AND MITIGATE E-FRAUDS

6.0 Introduction to e-security

The growing adoption of internet for business applications has exposed users to unwanted risks and attacks. Now more than ever, we find individuals/corporate houses exchanging critical information over the internet. However, lack of robust security infrastructure makes this information exchange vulnerable to outside intervention. To meet these challenges, businesses are opting for modern security measures, such as E-security. E-security measures are designed to preserve the confidentiality, availability, non repudiation and integrity of the users on the internet. The effective e-security requires a layering of multiple solutions focusing on people, process, technology and risk. Due to exponential increase in e-frauds since last decade, one needs to study the importance of e-security in this world of information systems.

6.1 Need for e-security

The need for E-security has to be dealt in different angles as e-frauds have many facets which are:

- Defacement of web sites
- Application vulnerability- loopholes in the software’s
- Site owner authored (accidental/intentional)
- Web server mis-configuration

An online transaction is a generally a web application comprised of a collection of programs/scripts, that reside on a web server and interact with a database and other sources of dynamic content. Runs generally at port 80/8080 on every computer. 70% of cyber attacks occur at application layer which is one of the Open systems Interconnect (OSI) layers where most programs runs. Data as part of legitimate traffic on port 80/8080 go undetected and conventional Network devices and firewalls cannot distinguish
bad data from the genuine data. Hence the web security is the prime concern of online service providers.

6.2 Web application security

This web application security refers to the following

- The combination of People, Processes and Technology
- Identify, Measure and Manage the risks while data moves in cyber space
- Open source and customized web applications

The risks are bound to occur due to various reasons. Some of the reasons are

- A malicious user can log in without a valid account.
- An unauthorized user views, adds, updates, deletes data.
- An authenticated user can add/update data as another user.
- A malicious user can upload malicious contents.
- A malicious user can steal user credentials.

To mitigate the risks the people-processes-technology matrix shown in Table 6.1 is recommended.

<table>
<thead>
<tr>
<th>People</th>
<th>Awareness</th>
<th>Training</th>
<th>Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processes</td>
<td>Secure Development</td>
<td>Secure code Review</td>
<td>Security Testing</td>
</tr>
<tr>
<td>Technology</td>
<td>Secure Configuration</td>
<td>Application Firewalls</td>
<td>Automated Scanners</td>
</tr>
</tbody>
</table>

This will improve e-security to a large extent. It is wrong to say that technology can cure all the problems. Even upgrading of software or hardware does not guarantee and safeguard from cyber attack.

However, while technology is a necessary condition, it is not sufficient to ensure success, especially in the area of cyber security. Without the
attention of well trained people e.g. cyber warriors/army, and without policies for e-governance and control of applications, IT networks are vulnerable for attacks from hackers.

Just think about how many networks are compromised because of “social attacks.” User receive an email from a source e.g. PayPal or a bank such as HDFC or SBI. The email looks real. It has no spelling errors and there is a link that looks like the real URL. But if we right click the link, the address of user message is in Nigeria, Romania, or even in a US city where the company doesn’t have any presence and the hackers who are waiting to get access to personal or company data and use this data for their personal gain.

Technology may be able to help to some extent in this circumstance, but in reality what is needed are policies and training of employees (and family members) to make them aware of cyber security and the variety of attacks. We need to train our security and network people to keep a vigilant eye on the traffic patterns to recognize the anomalies which are a precursor to new and different levels of attacks.

The third component that we need to address relates to policies. This refers to processes that are legitimately done at an organization. The number one area was professional and competent staff (the people factor) and the second – very close behind- was governance (policy). The technology factor was a distant third. As the matrix has impact on cyber security we have to have right mix of this matrix shown in Table 6.1 in any data processing organization.

Along with the people-policy-technology matrix, ever evolving web security standards should be adopted. To mitigate the risk involved in e-security the following plausible solutions are being used. They may mitigate the risk in certain concerned area and it is right mix of these solutions can meet robust e-security in this world of ever increasing cyber crimes. For example the web application security standards such as OWASP^52 (Open Web Application Security Project) and WASC (Web Application Security Consortium) are the two main standards being used in the web world. The OWASP is a project dedicated to sharing knowledge and developing open source software that promotes understanding of web application security. ^53 WASC is an international group of experts, practitioners and organizational
representatives who produce open source and widely agreed upon best practice security standards for the World Wide Web. As most financial online transactions are through web, the security of data in banking and financial institutions is vital to adoption of web security standards.

6.3 Overview of current financial enterprise

Today’s financial enterprise faces a daunting security challenge. It not only must build an impregnable fortress around its internal networks and applications, but it must also contend with the complications of sending and receiving encrypted data, and encrypting data at rest within application files and databases that were earlier not designed for secure handling of data.

Many banks that handle private or confidential data such as credit card and debit card numbers have the data stored in plain text in multiple locations throughout the bank. Typically a bank will have a large number of applications that process private or sensitive data that must be adapted to handle encryption.

There will be applications that handle ‘in sight’ data, sending and receiving data from other entities and applications that handle ‘static’ data, or data at rest. The applications are on a variety of computers with a number of operating systems, languages and databases and the computers are on multiple networks or subnets.

The encryption and decryption of sensitive data distributed throughout the financial enterprise requires a large number of resources – digital keys and digital certificates - that must be managed across applications, computers and networks in a cost effective and efficient way that does not compromise security. Additionally, user and application access to these resources must be controlled, managed and audited so that authorized access is quick and reliable, while malicious attacks are thwarted. To combat attacks newer procedures/practices were contrived and followed with meticulous security planning. These practices are

- Encryption
- Centralize Key Management
- Centralize Key Management with Localized encryption
- Centralize Key Management with tokenization
- Eliminate decryption/re-encryption Cycle for Key rotation or expiration
- Maintain Comprehensive Logs and Audit trails
- Use one solution to support field, File, database and backup storage

This financial scenario exists in every country. Providing security to user data is prime role of every organization doing business on the internet. Some of the e-security solutions which are successful and in vogue and that can be adopted to secure data on the transit in the network are suggested.

6.4 SUGGESTIONS

6.4.1 Suggestion 1: Alternate DNS Provider

Using an alternative Domain Name System (DNS) provider\textsuperscript{54}, such as OpenDNS or Google's Public DNS, can improve performance and increase security. OpenDNS is a DNS resolution service. OpenDNS offers advanced features, such as misspelling correction, phishing protection, and optional content filtering. There are several alternative providers. The importance of an alternative provider is to facilitate better browsing performance and enhance security, which can help to protect user from known phishing and malware-infected domains.

6.4.2 Suggestion 2: New Methods /Practices for Data Protection: Tokenization\textsuperscript{61}

As banks seek to protect data from cybercriminals, internal theft or even accidental loss, encryption and key management have become increasingly important and proven weapons in the security system for data at their end in databases, files and applications and for data in transit. Now there is a new strategy that adds an extra layer of data protection termed as Tokenization.

Tokenization is the process of replacing sensitive data with unique identification symbols that retain all the essential information about the data without compromising its security. Tokenization, which seeks to minimize the amount of data a business, needs to keep on hand for small and mid-sized
businesses to bolster the security of credit card and e-commerce transactions while minimizing the cost and complexity of compliance with industry standards and financial regulations.

Payment card industry (PCI) standards do not allow credit card numbers to be stored on a retailer's point-of-sale (POS) terminal or in its databases after a transaction. To be PCI compliant, merchants must install expensive end-to-end encryption systems or outsource their payment processing to a service provider who provides a "tokenization option." The service provider handles the issuance of the token value and bears the responsibility for keeping the cardholder data locked down.

In such a scenario, the service provider issues the merchant a driver for the POS system that converts credit card numbers into randomly-generated values (tokens). Since the token is not a primary account number (PAN), it can't be used outside the context of a specific unique transaction with that particular merchant. In a credit card transaction, for instance, the token typically contains only the last four digits of the actual card number. The rest of the token consists of alphanumeric characters that represent cardholder information and data specific to the transaction underway.

Tokenization makes it more difficult for hackers to gain access to cardholder data, as compared with older systems in which credit card numbers were stored in databases and exchanged freely over networks. Tokenization technology can, in theory, be used with sensitive data of all kinds including bank transactions, medical records, criminal records, vehicle driver information, loan applications, stock trading and voter registration.

6.4.3 Suggestion 3: 100% Adoption of Security Standards And 24x 7 Monitoring Of Standard

In evaluating the many options for network security solutions, it is essential to understand and consider the role of security standards. The growth in distributed computing and the ensuing increase in computer crime have led to legislation and regulations that establish legal requirements for network and data security. The various ANSI and ISO network security standards have undergone extensive peer review and represent the strongest security design thinking available in the commercial marketplace. Use of
standards compliant network security provides the best assurance of high quality, strong security for network, conforming to legal requirements.

6.4.3.1 Legal Considerations

There are now laws governing security of information in banking, corporate and government applications. The use of standards-based security is an important consideration in meeting legal requirements. In banking, there is very specific law requiring use of standards compliant security. For example, use of standards based systems protects banks against liability for electronic financial losses.

Commercially reasonable security standards have been defined by the international banking community through adoption of ANSI and ISO standards. These standards provide methods of data encryption; message authentication and user identification to protect against the risks encountered during electronic funds transfers. The adoptions of standards like PCI-DSS, EMV, etc., are being used as online security standards and are capable of protecting sensitive data.

6.4.3.2 PCI-DSS – 100% Compliant Framework

The PCI Security Standards Council was formed to work to secure payment account data in a globally consistent manner throughout the transaction process. Participating Organizations, which include merchants, payment device and service vendors, processors and financial institutions, play an integral role in the ongoing development of the PCI standards.

The PCI Security Standards Council was formed by the major payment card brands American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International to provide a transparent forum in which all stakeholders can provide input into the ongoing development, enhancement and dissemination of the Data Security Standard. Merchants, banks, processors and point of sale vendors are encouraged to join as participating organizations.

The Payment Card Industry (PCI) Data Security Standard (DSS) is a set of guidelines developed to help organizations that process credit card payments prevent credit card fraud, hacking and various other security issues.
A company processing, storing, or transmitting credit card numbers must be PCI DSS compliant or they risk losing the ability to process these payments.

The PCI DSS is a security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to assist organizations proactively protect their customer's information.

The core of the PCI DSS is a set of principles and accompanying requirements around which the specific elements of the Data Security Standards are organized as discussed in 4.5.1.

Even though most of merchants and financial institutions adopt PCI DSS, still the adoption will not be to extent it supposed to be there in place. Due to certain apprehensions towards financial transactions and budgetary constraints the banks/institutions are not fully compliant. Hence there is a scope of vulnerabilities which affect PCI-DSS compliancy. To have robust security total implementation of all security measures by PCI-DSS and run the transactions without any breach is essential.

6.3.3.3 Smart Card and EMV Standard

The smart cards can provide consumers with the ability to use the same card for numerous different transactions, unlimited by geography. Traditional credit cards have offered this convenience through adoption of global acceptance of brands such as VISA, MasterCard, American Express, and Diner’s Club, JCB, UnionPay, and others. Combining the convenience and security of smart cards with the widespread acceptance of such global brands is the obvious way to promote and increase in the use of smart cards.

To this end, EMV is a smart card payment standard designed jointly by Europay, MasterCard and VISA. The standard was established in order to build a standard platform for smart card credit and debit payment systems. It is anticipated that over the next 5 to 6 years, there will be transition from traditional magnetic strip cards to smart cards with an embedded chip. The Integrated Chips(IC) are able to calculate independently, encrypt and decrypt, and store information, greatly improving the security of card payments and reduce the risk of certain types of fraud, like ID theft fraud.
While ordinary smart cards have been widely accepted for a variety of daily transactions in Europe, US and urban China, EMV payment standard cards have only achieved limited penetration to date in India.

6.4.3.4 Migration to EMV Standard

Migration to the EMV standard from legacy magnetic strip cards is currently a large project within the global banking and credit card industry, and a key driver for this migration is the increased transaction and data security offered by the technology. With the development and widespread acceptance of the EMV standard, crimes such as credit card fraud (identity theft, and crime from stolen cards) which have exposed banks for many years are substantially reduced by the use of IC chips. This technology, which combines IC chips and a personal identification number (PIN), is a major development in the evolution of credit/debit card transactions. Since the EMV standard offers increased protection from fraud, in recent years credit card issuers worldwide have begun to transfer fraud liability to merchants using non-EMV compatible payment terminals, further spurring the adoption of the EMV standard.

6.4.4 Suggestion 4: Emergency Contingency Plan to Combat Shortcomings in the Security

Financial institutions are heavily regulated. They are required to implement security programs following regulations such as SOX, GLBA, SEC, HIPAA, PCI-DSS, ISO standards, etc. In fact, most of these organizations are required to execute an annual security assessment as a key compliance measure. Because an annual assessment may not discover all vulnerabilities, these organizations should be prepared to deal with security incidents involving physical facilities, network infrastructures, systems, applications, and most importantly, data.

Obviously, an entity that has no proactive mechanism to detect data, information, or system compromise wastes enormous amounts of time and money addressing an actual compromise without a response plan. To be able to deal with computer or IT related compromises, certain measures should be implemented by the institution. The following outlines example precautionary
steps recommended for a bank, but some of the measures are valid for any financial institution.

Under people, process and technology matrix banks can have greater security. This can be achieved by

- Proper planning
- Implementation,
- Monitoring and collecting response
- Identifying the security weakness with proper measurement
- Education and training for the employees and user
- Collect and preserve log data
- Institute an incident response plan
- Form an incident response team
- Train user about incident and reporting
- Forensics procedures to institute for possible litigation
- Create a forensic images of the suspected system
- Documentation of the scene
- Along the checklist the emergency contingency the monitoring of the online services is essential.

6.4.4.1 Credit Monitoring Services

Credit monitoring is a service which allows consumers to be advised about changes on their credit reports, and/or to view a summary of their credit report upon request. This service may monitor only one credit report or it could monitor reports from all the major Credit Reporting Agencies (i.e. Experian, Equifax and TransUnion). To date, credit monitoring products only help in a limited area of financial identity theft, and do not address the other forms of identity theft, such as criminal, governmental services, etc.

6.4.4.2 Identity Monitoring Services

These new services go beyond traditional credit monitoring by including additional areas where fraudulent activity may be indicated. In some cases, these may be more proactive in alerting you to fraudulent activity in real time.
6.4.4.3 Credit Freeze Products

A credit or security freeze is a stronger measure than a fraud alert. It literally locks your credit report from viewing for the purpose of new lines of credit, and for some employment and tenancy. When in place, potential creditors, insurance companies, landlords and some employers doing financial background checks may be told that your report is unavailable for viewing.

6.4.4.4 Data Sweep Services

This type of company checks the Internet for listings of your personal identifying information. While names, employee code and financial records are critical to identity theft, other pieces of information, such as your email address, also expose you to spammers and identity thieves. Once personal information is detected, these services will provide an alert so that steps may be taken to remove it.

6.4.4.5 Secure Payment Agents (SPAS) 64

A “Secure Payment Agent”, allows the consumer to control the use of all their sensitive personal information whether shopping, paying bills online, or registering at websites. A SPA has the ability to replace all of the user’s real personal information with anonymous data that becomes useless after a transaction and cannot be tracked back to the user.

6.4.4.6 Identity Theft Insurance

These are insurance programs, or add-ons to existing policies, that help replace real expenses incurred by the victims of identity theft.

6.4.5 Suggestion 5: E-Lock Digital Signature 65

E-Lock digital signature solutions provide the basic e-security foundation for businesses. Along with authenticity, the solutions make sure that the information or transactions are not intercepted and exploited. The solutions are designed to suit the business requirements of the user, making them user-friendly. E-Lock facilitates a secure and safe business environment
for its users, which allows them to conduct business operations freely. With reduced time spent on security concerns, users can divert their focus on business expansion activities.

This E-lock solution can be easily integrated into applications, such as document management, core banking, workflow management, e-mortgage and e-tendering, without disturbing the current workflow. This leads to a win-win situation for the customers, as they do not have to pay extra to make solutions compatible with their existing ones. Hence, compliance is guaranteed in a cost-effective manner.

With E-Lock solutions, customers can encrypt and digitally sign files in any online format. This encrypted message can be mailed/stored while assuring the data integrity. In order to conduct data verification and authentication, customized settings are provided to allow only authorized persons to access that data, maintaining privacy and security.

At present, the Railway Infrastructure Corporation (Australia) uses E-Lock DeskSeal Web to boost its e-security. The solution is used to approve sensitive designed documents, and all communication is encrypted to ensure privacy.

Other benefits can be had with E-Lock are:

- Improved security measures
- Data integration
- Legal compliance
- Reduced overhead
- Less processing time
- Effective time management
- Growth environment

6.4.6 Suggestion 6: Creating A IT Security Checklist

IT policies have undergone considerable changes the since last decade to accommodate changing IT environments, and increased emphasis on information security. In addition to digital information, all information in the
bank should be included. With regard to digital information, we offer the following check-list:

- Outer wall or first line defense: fire walls.
- Designate firewall to be used. (make, model)
- Who is to have access to firewall?
- How often are settings to be reviewed?
- Document reviews
- Second line of defense, access to network
- Who has access to network?
- Physical access
- Logical access
- Set levels of access for those with access
- Administrative rights
- Read, write access
- Read only
- Password requirements
- Time network available

To further strengthen the existing security, additional check list may include:

- Applications: Specify acceptable applications on network.
- Set level of security for each application.
- Core processing, set levels of access within core processing applications, password requirements
- Other Applications - who has what access
- Review usage reports, and document reviews for unusual and improper access.

6.4.7 Suggestion 7: Biometrics Adoption

Biometrics can provide a key element of identity management, both in terms of biometric user authentication and identity assurance systems. In the area of cyber security, it is important to know both who is attempting to access a system and that biometric identity data is itself protected. Biometrics has
emerged as an important tool in supporting effective identity management by strongly binding a physical person to their identity.

Most computer breakin’s today are due to compromise by system users or hackers who use legitimate accounts to gain access to general security. Determining the identity of a person is becoming critical in our widely connected information society. As a large number of biometrics-based identification systems are being deployed for many civilian and forensic applications, biometrics and its application have evoked considerable interest.

Biometrics comprises methods for uniquely recognizing humans, based upon one or more intrinsic physical or behavioral traits. In computer science, in particular, biometrics is used as a form of identity access management and access control. It is also used to identify individuals in groups that are under surveillance.

**Biometric characteristics can be divided into two main classes:**

Physiological are related to the shape of the body. Examples include, but are not limited to fingerprint, face recognition, DNA, Palm print, hand geometry, iris recognition, which has largely replaced retina, and odor/scent.

Behavioral are related to the behavior of a person. Examples include, but are not limited to typing rhythm, gait, and voice. Some researchers [1] have coined the term behaviometrics for this class of biometrics. Strictly speaking, voice is also a physiological trait because every person has a different vocal tract, but voice recognition is mainly based on the study of the way a person speaks, commonly classified as behavioral.

Biometrics -- technology that uses the human beings’ physical or behavioral traits for identification purposes -- will play an important role in the near future of desktop computing, mobile phones, and, in particular, access to institutional computers and sensitive data via the Internet.

Biometrics provides greater protection of our personal data and financial assets, which is more essential than ever before. Biometrics can better safeguard our most critical data that could cause us the most harm if accessed by the wrong person. Some of the biggest potential applications include the use of biometrics for access to Automated Teller Machines (ATM) or for use with credit or debit cards and as a general use for combating credit
card fraud. Many types of financial transactions are also potential applications e.g., banking by phone, banking by Internet, and buying and selling securities by telephone or by Internet.

Implementing payment processing systems that utilize biometrics with private account management can easily prevent credit card crime. Biometrics can be incorporated at the point of sale, thereby enabling consumers to enroll their payment options e.g., checking, credit, debit, loyalty, etc., into a secure electronic account that is protected by, and accessed with, a unique physical attribute such as a fingerprint. Cash, cards or cheques are not needed to make purchases, so there is no need to carry them in a purse or wallet. Not carrying a purse or wallet eliminates the chances of it being stolen or lost while shopping.

Biometric transaction-processing systems allow consumers to manage point-of-sale payment easily and securely. This solution is particularly well suited for personal check use. Biometrics can also offer increased protection for check-cashing services, whether personal or payroll. By requiring biometric identity verification before allowing a check to be cashed, the possibility of it being presented by anyone other than the intended payee is eliminated.

6.4.8: Suggestion 8: Artificial Intelligence, Fuzzy Logic And Neural Network in Cyber Security

6.4.8.1 AI Firewall for Network Security

Artificial intelligence applications are uniquely suited for the ever-changing, ever-evolving world of network security. Typical firewalls are only as good as the information provided by the network administrator. A new type of attack creates vulnerabilities, which a static firewall does not have the ability to avoid without human direction. An AI-managed firewall service, however, can protect a computer network from known and future threats.

6.4.8.2 Network Security Solutions using AI

Network security solutions are often very expensive, and must be frequently upgraded in order to keep up with changes in intrusive techniques and technologies. An artificially intelligent firewall is constantly upgrading its
knowledge base in response to events, and increasing its protective abilities, which may forestall the need for constant updates. Using artificial intelligence applications to enhance network security solutions requires both initial training and experience for the firewall.

6.4.8.3 AI to Secure Network Access

A firewall is necessary in order to limit network access to only authorized applications and access requests, while allowing legitimate information requests. Without protection, a network is vulnerable to the outside world, and may be accessed by hackers or computer programs. Using artificial intelligence to improve the performance of a firewall ensures that the protection provided by the firewall improves over time, in reaction to changes in threats and attacks.

6.4.8.4 Fuzzy Logic Applications for Banking and Loans

Fuzzy logic enables a computer program to arrive at a decision based on multiple factors with different levels of importance. Rather than "yes" or "no" answers, this type of decision-making software deals with "maybe" and "sometimes". During the decision-making process, this type of artificial intelligence (AI) program evaluates weighted factors to reach a conclusion.

Lenders use a complex set of criteria in order to determine whether to approve home mortgage loan applications. These decisions have traditionally been made by loan officers, after a careful evaluation of loan applications, credit history, work history, and other factors. Now, however, fuzzy logic applications are being used to make this process easier and more efficient for lenders.

Each factor that applies to the decision made by the fuzzy logic application will have a "weight", or level of importance, assigned to it. The application will compare not only the positive or negative results, but the relative importance of each result. The calculations required to process each decision can be extremely complex. AI applications performing fuzzy logic calculations often use neural networks for processing power.
6.4.8.5 Artificial Neural Network (ANN)

Artificial neural networks bring a number of critical competitive edges to traders, portfolio managers and trading managers. For traders, they provide a useful early warning of changing trends. For portfolio managers, they provide a faster, more accurate way of screening and selecting securities. For trading managers, they provide a way of improving overall performance, of benchmarking results against a standard customized to their particular risk profile, of monitoring compliance, and of detecting fraud (Caudill and Butler, 1992).

In Kingdon’s (1995c) paper, the author describes how the establishment of artificial neural networks were used for fraud detection in merchant banking (Fidelity Investment, Citibank), marketing (Thorn-EMI, American Express-Amex), retail banking, and insurance (TSB).

Another report by Card World Publications, (1994) maintains that artificial neural networks are largely responsible for reducing fraud substantially for Visa International. According to Northants (1994) report, ‘initially the system was trialed in five Canadian and ten US banks, whose customers numbered 40 million card holders. The neural network was ‘trained’ to spot fraudulent activity by comparing legitimate card usage with known cases of fraud. By using patterns based on aspects such as the time of transaction, the frequency of transaction, the size of transaction, or the type of transaction (i.e. the merchant type) a comparison could be made to an existing model held for each individual cardholder. Once a pattern of behavior was judged by the system as unusual, or potentially fraudulent, the system sounded an alarm, and the transaction was investigated further (Card World Publications, 1994).

In another report by the Intertek Group, a fraud detection system called ‘Card Risk Identification Service (CHRIS)’ has saved an estimated US $18 million for Visa International. The system was able to handle 20 million authorizations a day (Intertek Group, 1994).

Intertek Group (1994) points out that Hecht-Nielsen Neurocomputer Corporation (HNC) Software is one of the largest suppliers of artificial neural net-based credit card fraud detection software. HNC’s Falcon system is used by thirty credit and transaction card suppliers world-wide, and monitors over
90 million accounts. According to HNC, users of Falcon save on average 25% more through avoiding losses resulting from fraud than other users achieved by alternative existing strategies (Intertek Group, 1994).

The above reports supports the fact that a right combination of Artificial Intelligence, fuzzy logic and neural network would play major role in anticipating, detecting cyber frauds in any form. Thus effective e-security requires a layering of multiple solutions focusing on people, process, technology and risk.

6.4.8.6 Recommended Ultimate high security model

After the study of various security methods adopted and the analysis of cyber frauds in the financial sector from 2009-2010, the following Basic-Biometrics-Behavior metrics(BBB) Security Model is developed for robust and high secure online transactions is as shown in figure 6.1, 6.2 and 6.3.
Ultimate high Security Model

This Basic-Biometrics-Behavior metrics (BBB) model can give 99.9% secure online truncations as it involves user knowledge, physiological traits along with behavior which adopts artificial intelligence, fuzzy logic and neural network to identify any online transactions by a human being. This ultimate high secure model will make fraud free online transactions on the network. The cyber frauds can occur due to weakness and vulnerability in the basic model. Over the period with technology developments different techniques were tested to reduce the cyber frauds. In this faster communications and high speed computation the BBB model might reduce the frauds on the network substantially.