Securing Mobile Banking In Intelligent Mobile Devices - Pattern Based Authentication Approach

S. Dedeepya, P. Swetha and Y. RAJU

Abstract — Mobile banking has emerged as a powerful provider of banking services offering easy access and plentiful applications for smart phones. Due to the increase in the use of mobile banking services, mobile banking has become an attractive target for attackers. Customers and services provider's face various threats in mobile banking, in spite of security measures taken by current mobile services. Some threats against mobile devices such as physical theft or penetration from the remote side are still unsolved. This paper proposes a novel approach to prevent such threats by analyzing the input patterns of mobile banking users such as how long it takes a user to input data into a mobile device, the normal finger pressure levels and physical touch dimensions when using a touch screen. We can distinguish the differences between an actual user's usage pattern and an attacker's usage pattern. The empirical results revealed that the system is highly accurate and effective which can be used in real time systems.

Keywords-Banking security; input pattern recognition; mobile authentication; biometric; neural network

1. INTRODUCTION

The rapid growth and innovations in mobile technology and growing importance of mobile capabilities in the lives of the consumer led to the evolution of mobile phone into a mobile banking transactional and payment instrument. This challenged the existing security features on mobile devices. McAfee's 2009 mobile security report revealed that mobile banking is the highest security concern for mobile device manufacturing companies [1]. Newly-discovered mobile malware in 2010 amounted to ten million, which was a rise of 46 percent from a year ago, and various vulnerabilities continue to be founded in Symbian, iOS, and Android mobile platforms [2]. In addition, mobile phishing attacks using Multimedia Messaging Service (MMS) or QR code have been materializing [3]..

As usage of pc based security measures in online banking cannot be incorporated directly into the mobile device's keeping in view of mobile device's battery life, computing power and bandwidth availability [4]. So now the time is ripe for emergence of new authentication methods to be made available on all mobile devices equipped with mobile banking application so as to enhance security.

In this paper, we proposed a pattern-based authentication method (IPAM) for securing mobile banking in intelligent mobile devices. The proposed method concentrates on mobile devices with touch screen as the input medium which receive input through fingers or stylus, as many mobile devices adopt touch screens as their input medium. In this regard we measure the user's usage patterns such as the input duration-time, finger- pressure level and physical touch dimension on the touch screen. The minimum time required by a user in providing input is considered for measurement while doing so the amount of pressure applied on the touch pad is also correlated with the dimension of his/her finger in contact with the touch pad. These above three measurements are consistent and distinct from those of other users. These features of quantified user's input patterns can be used to identify users and detect an illegal transaction by an attacker. Even though there could be a chance for the password to be leaked to an attacker after being successful gaining the rights as the user the proposed method (IPAM) still holds back the user in proceeding forward with his attack by analyzing the differences in input patterns between the legal user and an attacker.

Biometric authentication is the most sought after technique for its wide scope in usage of Fingerprints, hand geometry, facial recognition, iris scanning and voice prints [5]. In particular, a mobile device, which is equipped with a camera, a microphone, and a touch screen, facilitates multimodal biometric authentication. [6]. These methods, however, have the following drawbacks. First, they can be compromised by biometric spoofing attacks. Many attack methods like fake plastic fingers have already been reported and proven to effectively evade biometric authentication systems. [7]. Second, the additional work for authentication inconveniences users.

Third, a high storage capacity is required to keep a large volume of scanned biometric data. Fourth, the collection of personal biometric information can cause privacy infringement trouble to banks or financial institutes. In order to overcome above problem, the biometric authentication method which utilizing keystroke pattern was proved to have high error rates that is approximately 21% [8] [9], due to its dependency on a behavior attribute which is more variable than a physical attribute. Also, keystroke patterns frequently change when ever a user establishes a new password i.e., the rate at which the user give the password as input varies from time to time. Furthermore, this method is applicable only for the old phones (so called feature phones) without a touch screen.

Taking above facts into consideration, existing biometric authentication methods are not suited for the current mobile banking environment that utilizes intelligent mobile devices. IPAM, on the other hand, has the following advantages over other biometric methods. First, it is capable

S.Dedeepya, P.Swetha and Y.RAJU are with GCET, JNTUH University, Emails: sdedeepya@gmail.com, chaithna@gmail.com, Raju.yeligeti@gmail.com

of preventing spoofing attacks. In order to avoid the explicit operations like fingerprint and scanning in biometric authentication methods we adopt the IPAM which facilitates the collection of user input patterns spontaneously during mobile banking procedures. Therefore the spoofing attacks which were possible in biometric authentication are avoided in IPAM as the attacker is unable to track the information to be collected for authentication. Second, the input pattern data using a text-based format needs much less memory compared with scanned images or voice data. Third, IPAM guarantees a high accuracy rate. This is because it combines a user's behavior attributes with physical attributes. Fifth, IPAM does not infringe on a user's privacy at all in contrast to other biometric information.

To evaluate the efficiency of IPAM, we experimented with a practical personal input pattern data set. We firstly collected user's input patterns through a self-developed mobile application on major Smartphone platforms. Next, we trained with the collected user's input pattern data and evaluated how accurately IPAM could verify a user's identity. The training and classifying algorithm applied a back propagation network (BPN), which is a neural network using a supervised learning method and a feed-forward architecture [10]. Our experimental results show that IPAM is capable of effectively identifying mobile banking users at an accuracy rate of over 98% in our tests.

II. THE ISSUES OF MOBILE BANKING SECURITY IN INTELLIGENT MOBILE DEVICE

1.The Trend of mobile banking Incidents

Accessing online bank accounts from mobile devices has increased from 23 percent in 2010 to 54 percent in 2012.The mobile banking has become an integral part of banking sector in many countries. It is not different in Korea. The reports of FSS(Financial Supervisor Service) in Korea reveals that thirteen incidents occurred each year from last five years and the number of damages reached to more than 290 million so far. Most mobile banking incidents occur on attacking user PCs, not the e-financial system. This is due to the vulnerabilities in the PCs rather than mobile banking systems. It does mean that applications used for transactions are secure.

However, the device in which applications are running is having security vulnerabilities. This is the case with both PC and Intelligent mobile devices. For this reason financial systems undergo periodic vulnerability checking and around-the-clock security monitoring. On the other hand user mobile devices have a high chance to be attacked because of insufficiency in basic security measures such as running antivirus program or applying security updates for PC's or Intelligent mobile device's operating system.

2. The Internet Banking Security Protection Methods

In Korea, with respect to user authentication and digital signature, the financial institutions utilize digital signatures and one time pad that guarantees a user's identity and integrity of transactions. The digital certificate, as a digital signature technique with PKI (Public Key Infrastructure) plays an important role in authentication and non-repudiation of most online banking services thereof safeguarding the interests of the stakeholders involved in the mobile banking transactions. Among the one time pads, a security card which contains about 30 different password codes each with 4 digit number which change for each transaction, is popular. The limit in the number of password codes being a drawback for a security card can be replaced by a random password generating device for providing additional security. With respect to the protection of user's authentication information mobile banking systems installed security software's in intelligent mobile devices for malware detection, access control, message encryption, and key-logger protection.Inspite of taking all this measures the mobile banking systems are not able control attacks like memory hacking.They are still desperate to find more effective solutions to these problems Another method for authentication is based on the information in mobile device/PC.As the user mobile devices are not under the control of mobile banking systems they are not considered as trusted devices. Hence it is hard to protect user's authentication information during transactions in mobile devices.Identifing these problems, the banking institutions developed a user's mobile information based authentication methods for mobile banking to distinguish between legal user's transaction and an attacker's transaction.

For this method, mobile banking systems made use of PC based information such as geolocation, MAC address, and its serial number. For example ,if the transaction on a PC located at A is requested from a banking account which mainly does transactions on PC located in B, mobile banking institutes can consider this transaction as suspicious.

This approach is likely to be an effective counter measure against mobile banking incidents because it is possible to block illegal transactions even when all authentication information is known to attackers.Inspite of taking all this measures security is compromised if attacker disguises their PC information as the original user PC's. In addition, the privacy infringement problem caused by the collection of user PC information is another task to be solved.

As the current mobile banking service includes most internet banking services such as balance checking, account transfer, payment, and other banking conventional banking services, mobile banking security protection methods plays a prominent role. Additionally device platforms for mobile banking are based on operating systems used in PCs like Windows and Andriod.Thus the security threats of Internet banking such as malware and phishing attacks will happen in mobile banking as well[12]

For this reasons, the Banking supervisor service advised of financial institutes to apply the same level of security measures should be applied for mobile banking as internet banking, like using the digital certificates and installing security software. By taking into consideration of above policy banking institutes have been operating mobile banking with nearly equal security measures to Internet banking, even though mobile devices have restricted performance.

However, still exists the possibility of leaking a user's authentication information for transactions in mobile banking. The mobile device is a non-trusted device which resembles a PC. Furthermore, a mobile device has a higher chance of malware infection due to a more varied infection route than a PC such as MMS, Bluetooth, and PC-sync. It is conceivable that the authentication method using mobile device information such as International Mobile Equipment Identity (IMEI) and Global Positioning System (GPS) information, is a good alternative. It is, however, expected to have identical problems to a user PC information-based authentication method. Firstly, GPS information is basically included in the area of personal information. Therefore, financial institutes can use GPS information for authentication only if they get the approval of users, but otherwise they may face the privacy infringement problem. Next,like PC information, mobile device information is also easily leaked to attackers by mobile malware. Once attackers disguise their information as the original users', a mobile device information-based authentication method can be compromised.

III. USER'S INPUT PATTERN-BASED AUTHENTICATION METHOD

A. Basic Principles and Architecture

Touch screens are the main interface device for a smart phone because of its small size and difficulty to attach physical input devices like a keyboard and mouse. Therefore, mobile banking users use a finger as a part of the body to input (touch and scroll-wheeling) in the process of the transaction. In this case, a user's input pattern such as an input duration time, finger-pressure level and physical touch size on the touch screen could be considered as one of the types of biometric authentication information. The biometric authentication information, which would be based on fundamental human characteristics, could be used not only for checking whether or not a person exists, but also for verifying a user's identity. Liang Xie et al., recently, describe that input patterns on mobile devices can be used to detect a simulated input by malware which is posing as a human user [13].

Based on these ideas, we proposed a novel authentication method using a user's input pattern, named as IPAM, for preventing mobile e-financial accidents. There are inevitably differences in input patterns among mobile banking users because each user has unique biometric features such as the specific finger used, finger size, and various input behavior attributes. Thus, by analyzing a user's input pattern, financial institutes can detect illegal transactions by attackers who are not the original user, even when the user's authentication information for transactions in mobile banking is intercepted by attackers.

Fig. 1 shows three phases of IPAM architecture: training, detection, and countermeasures. In the training phase, as advance preparations, IPAM initially collects the user's input pattern data, and then this data is transferred to the e-financial system and stored in a database for training.

Next, IPAM standardizes a user's input pattern by training several times with the collected data. The training needs a certain level of operation, so it is proper to perform the training in the e- financial system, rather than in the resource-constrained mobile device. Furthermore, carrying out the training in the e-financial system guarantees security and helps to prevent possible damage of training integrity from mobile malwares installed on a Smartphone.

The detection phase is for making a decision, whether a requested transaction is the original user's or an attacker's. If the input pattern of the requested transaction is not similar to one already registered by training, financial institutes can consider this transaction as a suspicious one performed by attackers. In this case, financial institutes will not approve this transaction, and then execute an additional authentication process.

The countermeasure phase is for executing secondary authentication processes for suspicious transactions detected. The financial institutes can clearly check and block illegal transactions by attackers with this procedure. In this paper, we excluded detailed methods for the countermeasure from our discussion.

B. Components and Implementation

There are two types of input methods in the process of mobile banking: touch and scroll-wheeling. The touch is an input mode to press mobile widgets like a button with the finger. And the scroll-wheeling is the action of brushing a finger up or down on the touch screen to shift positions. These touch and scroll-wheeling patterns can be different for each user, according to a user's physical and behavior attributes. Table 1 represents the attributes used to influence a user's input pattern.

As seen in Table 1, physical and behavioral attributes affect a user's input pattern, so there is little possibility of the existence of two users with similar input patterns.

Figure 1. The three steps of IPAM architecture: training, detection, and countermeasures

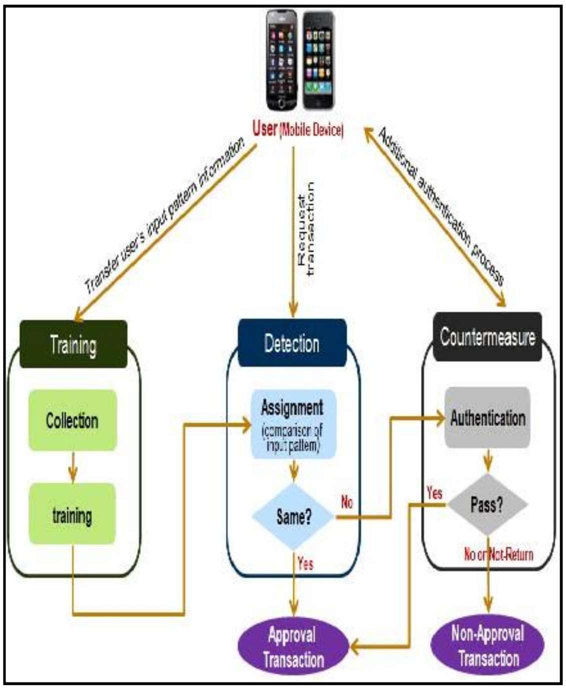


TABLE I:-ATTRIBUTES AND USER'S INPUT PATTERN.

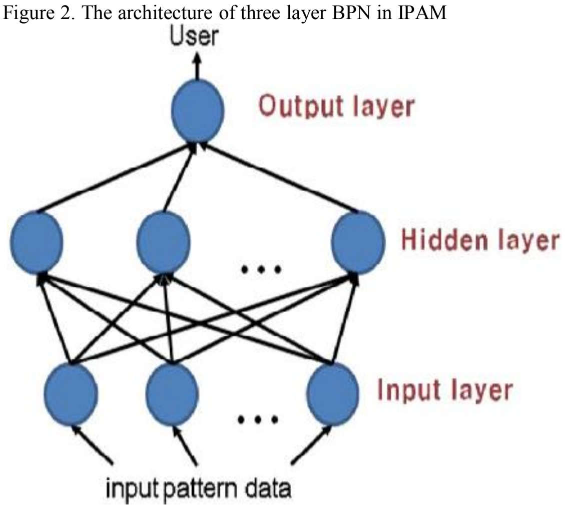
Attributes	**User's Input Pattern**	
Using Hand	Left Hand	Right Hand
Using Fingers	One Finger	Multi Fingers
	Thumb	Index Finger

Touch & Scroll-wheel *Duration time*	Long	Short
Touch & Scroll-wheel *Pressure level*	Strong	Weak
Touch & Scroll-wheel *Dimension*	Wide	Narrow
Scroll-wheel *Position* (Start and End)	Variety (Top, Bottom, Left, Right)	
Scroll-wheel *Speed*	High	Low
Scroll-wheel *Length*	Long	Short

In this sense, IPAM can be effectively used in identifying mobile banking users for prevention of mobile e-financial incidents.IPAM uses the Back Propagation Network (BPN) to train user input patterns. BPN, by using Least Squares Method (LSM), is the most widely used neural network algorithm in pattern recognition [10]. One of the biggest reasons to propose BPN as a training algorithm is that BPN has a better fault-tolerance capacity than other algorithms for training [14]. It is difficult for a person to always input in the same way that a machine would. Thus, noisy input values could rarely be included in user input patterns. BPN, however, is able to reduce a training error on account of its superior fault-tolerance, even though some noise is contained in the data.

An Architecture of BPN, three layer networks with one hidden layer is shown in Fig 2. The input layer consists of processing nodes for user's input pattern data. Thus, the total number of processing nodes in the input layer is equal to the number of user's input pattern data elements. The number of processing nodes in the hidden layer deeply influences the accuracy and performance of training. The transfer function equations for each processing node are provided for both forward and backward passes.

Figure 2. The architecture of three layer BPN in IPAM



A. Experimental Setting and Configuration

The number of Linux-based smartphones has substantially grown in recent years. For this test, we chose a Motoroi, a Linux-based smartphone. The Motoro includes Android 2.1

OS and a 3.7 inch touch screen. To collect user input patterns, we developed a separate mobile application for testing, and then installed this application on the Motoroi. The Application Program Interface (API) of Android gives special classes for collecting input patterns, for example, the View.MotionEvent class. In this test application, we arranged 18 button widgets for touch input test in different locations as seen in Fig 3. This is because some user's touch input patterns can be varied by a widget's position. The scroll-wheeling input test followed a touch input test.

A total of 50 persons in their 20s and 30s, which were familiar with mobile devices, participated in our test, and each person performed the touch and scroll-wheeling test 10 times. We did not disclose the aim of this test to the participants because if the participants knew what information was being collected in the test, the results were likely to be affected. The user's input pattern attributes collected for training were as follows: {touch(3) : Duration time, Pressure level, Dimension} {scroll-wheel(9) : Duration time, Pressure level, Dimension, Start-Position(x,y), End-Position(x,y), Speed, Length} he training algorithm adopted BPN and set up the following configurations – the number of hidden layers : 1, activation function : sigmoid, the initial weight value : random value within -0.3 ~ +0.3, training stop condition : iteration number 10000 or Mean Square Error (MSE) 10^{-7}. Training executed in a PC environment included a 1.3Ghz CPU and 3G memory.

Figure 3: the picture of application for touch input test

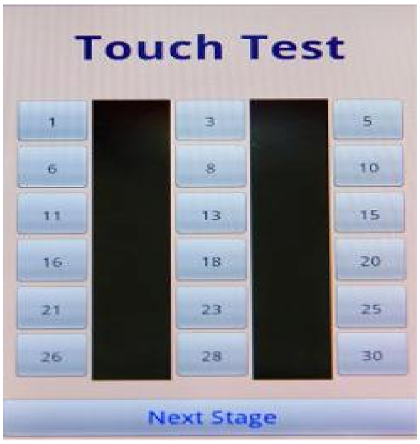


TABLE II. THE TEST RESULT OF 50 USERS.

Variable	Input node number	12				10			8
	Hidden node number	**12**	**10**	**8**	**6**	**10**	**8**	**6**	**8**
Result	Accuracy rate (%)	97	97.6	95.8	90.2	96.2	91.6	88.4	88.6
	Iteration number	4705	5198	7141	10000	5714	7288	10000	7653
	Train time	5:46	4:32	5:38	4:52	3:45	4:03	4:28	3:55

B. Experiment Results

In this test, we evaluated how correctly 50 users were classified with the trained input pattern, as changing the number of input and hidden nodes of BPN.

Table 2 represents the test result regarding 50 users. The state of 10 hidden nodes generally brought about better accuracy rates and performance than other states. The accuracy rate of 12 input nodes and 10 hidden nodes was the highest level, 97.6%, and the accuracy rate in the lower 8 hidden nodes was below 90%.

Fig. 4 shows the difference of training graphs between 10 hidden nodes and 6 hidden nodes in the case of 12 input nodes. Even though the accuracy rate in both graphs continued to be enhanced in proportion to the iteration number, the graph describes that the accuracy rate in 10 hidden nodes was higher than that in 6 hidden nodes. Even if we tried to increase the iteration number from 10000 to 50000 in 6 hidden nodes, the accuracy rate was not enhanced at all.

We used a deviation coefficient (DC), the distance from an average, as criteria to decrease the number of input nodes. If an input attribute had a relatively high DC value, then it was thought to have more noise input than other attributes. Therefore, the attributes of high DC were not proper to apply to user's authentication.

TABLE III. THE DC OF ATTRIBUTES IN 50 USER'S INPUTS

Attributes		**Average of**	**Large Order**
touch	Duration time	0.76139	7
	Pressure level	0.77436	4
	Dimension	0.69039	12
Scroll - wheel	Duration time	0.75683	9
	Pressure level	0.77808	3
	Dimension	0.78356	1
	Start-	0.74611	10
	Start-	0.76094	8
	End-	0.78256	2
	End-	0.76531	5
	Speed	0.76437	6
	Length	0.74074	1

As seen in Table 3, there was no great difference of DC between the input attributes, and the large order of DC was asfollows: Scroll-wheel Dimension, Scroll-wheel End-Position(x), Scroll-wheel Pressure Level, and Touch Pressure level.

Consequently, our test results demonstrated that IPAM had the ability to identify mobile banking users with high accuracy rates. The accuracy rate of IPAM (about 98%) could be regarded as very high considering the accuracy rate of other biometric authentication methods (91 ~ 98.5%) [8].

In addition, we found that the DC of the initial attempt among ten overall attempts in testing was nearly twice than the DC of other attempts. This is because users were not accustomed to the test application during the initial attempt. We experimented without the initial attempts, and obtained a higher accuracy rate (about 99%) and better performance as shown in Table 4. In this sense, if the financial institutes would train a user's input pattern without the beginning transactions in mobile banking, IPAM will have more efficiency.

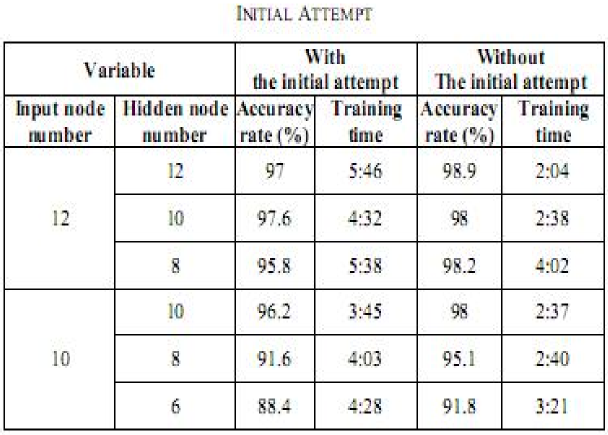
V. CONCLUSION

Each banking institution with online mobile access is starting to implement portals with the aim of seducing both clients and prospects by combining services that are accessible to all and functions that require valid authentication. soon, because it is more convenient [12] and since mobile phones are continually being improved, the services on offer continue to evolve so that you can now perform a large number of tasks from your mobile phone as well as being able to freely manage your accounts when it best suits you

This paper proposed a novel authentication method for mobile banking by analyzing a user's input pattern (IPAM), and we demonstrated through practical experiments that IPAM was an effective method for preventing mobile banking incidents. Our approach also guaranteed high accuracy, easiness to deploy without high cost, a real hardship for malicious attackers to forge, and no infringement of privacy.

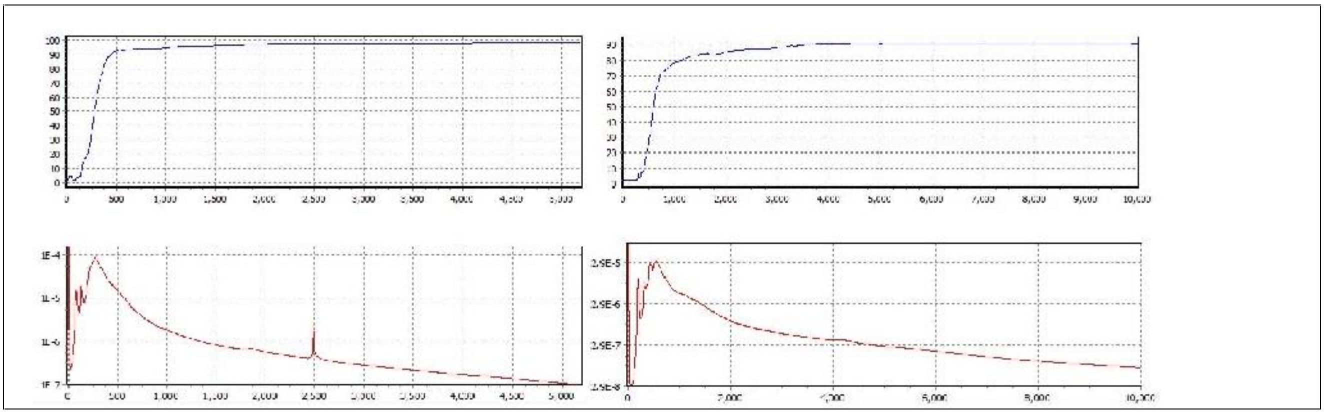
In the immediate future, we foresee that the mobile environment and device techniques will have more diversity. In this regard, there is a need to improve our IPAM considering these changes. These remaining issues are our future work.

TABLE IV. THE ACCURACY RATE AND PERFORMANCE WITHOUT THE INITIAL ATTEMPT



INITIAL ATTEMPT

Variable		With the initial attempt		Without The initial attempt	
Input node number	Hidden node number	Accuracy rate (%)	Training time	Accuracy rate (%)	Training time
12	12	97	5:46	98.9	2:04
	10	97.6	4:32	98	2:38
	8	95.8	5:38	98.2	4:02
10	10	96.2	3:45	98	2:37
	8	91.6	4:03	95.1	2:40
	6	88.4	4:28	91.8	3:21



10 Hidden Nodes] **[6 Hidden Nodes]**

Figure 4. The comparison of training graph between 10 hidden nodes and 6 hidden nodes in the case of 12 input nodes.

References

[1] "Mobile Security Report 2009," McAfee, www.mcafee.com, 2009

[2] McAfee Threats Report : Fourth Quarter 2010", McAfee, www.mcafee.com, 2010

[3] "XSS, SQL Injection and Fuzzing Barcode Cheat Sheet," ttp://www.iro ngeek.com/xss-sql-injection-fuzzing-barcode-generator.php

[4] Aubrey-Derrick Schmidt, Frank Peters, Florian Lamour, Christian Scheel, Seyit Ahmet Camtepe, and Sahin Albayrak, "Monitoring Smartphones for Anomaly Detection," Mobile Network and Application, 2008, pp. 92-106

[5] N.L Clarke, and S.M furnell, "Authentication of users on mobile telephones – A survey of attitudes and practices," Computer & Security, vol 24, 2005, pp. 519-527

[6] J.Koreman, A.C Morris, D.Wu, S.Jassim, H.Sellahewa, J.Ehlers, G.Ghollet, G.Aversano, H.Bredin, S.Garcia-Sallicetti, L.Allano, B.Ly Van, and B. Dorizzi, "Multi-modal biometric authentication on the SecurePhone PDA", in Proc. 2nd Int. Workshop Multimodal User Authentication, Authentication, Toulouse, France, 2006.

[7] Chris Roberts, "Biometric attack vectors and defense", Computers& Security, vol 26, 2007, pp. 14-25

[8] N.L Clarke, and S.M furnell, "Advanced user authentication for mobile devices," Computer & Security, vol 26, 2007, pp. 109-119

[9] Seong-seob Hwang, Sungzoon Cho, and Sunghoon Park, "Keystroke dynamics-based authentication for mobile devices," Computers & Security, vol 28, 2009, pp. 85-93

[10] Robert Hecht-Nielsen, "Theory of the Backpropagation Neural Network," IEEE Neural Networks, 1989, pp. 593-605

[11] Petr Hanaeek, Kamil Malinka, and Jiri Schafer, "e-Banking Security – A Comparative Study," IEEE A&E SYSTEMS MAGAZINE, vol 25, 2010, pp. 29-34

[12] Jin Nie, and Xianling Hu, "Mobile Banking Information Security and Protection Methods," Computer Science and Software Engineering International Conference, 2008, pp. 587-590

[13] Liang Xie, Xinwen Zhang, Jean-Pierre Seifert, and Sencun Zhu, "pBMDS : A Behavior-based Malware Detection System for Cellphone Devices," WiSec'10, 2010, pp. 37-48

[14] Jay I. Miinnix, "Fault Tolerance of the Backpropagation Neural Network Trained on Noisy Inputs," IEEE Neural Networks, 1992, pp. 847-852

She completed BTech,MTech from JNTU,Worked as Asst professor in Dept of IT at GCET, Hyderabad.She published 2 international journal publications.

She completed BTech, MTech from JNTU,Worked as Asst professor in Dept of IT at GCET, Hyderabad. She published 2 international journal publications

Worked as Associate professor in IT Dept at GCET. Hyderabad..He received BTech ,MTech from JNTU. Presently Pursuing Ph.D from JNTU.He published 9 international journal publications. He published 4 international conferences.