Towards Digital India Transformation: Pragmatic Implementation of 3 Dimensional Cyber Security Pyramid to Counter Cyber Attacks in India

Cosmena Mahapatra
Asst. Professor, VIPS, GGSIPU, New Delhi, India.

Meenu Chopra
Sr. Asst. Professor, VIPS, GGSIPU, New Delhi, India.

Abstract – Digital India is a dream that every Indian supports. This has not only made life easier but also transparent thus paving way for a corruption free future. However recent cyber-attacks have raised awareness in Indian digital word for more pragmatic anti cyber terrorism course of action. These may encompass techniques such as Machine Learning and Sentiment Analysis. This paper presents a three dimensional architectural view of implementing various IT policies and techniques which assure a safe cyber future and a smooth digital transformation in India.

Index Terms – Cyber Attacks, Machine Learning, Sentiment Analysis, Digital India, MLP, ANN, Data Mining.

1. INTRODUCTION

Digital India [1] is a transformation which is paving way for a corruption free society and is putting India onto the level of developed Countries of the world. Indian Government and Cyber experts are working 24*7 to make India an impeachable digital fortress yet India still has a long way to go before this dream is fully achieved.

Let us first understand what is a cyber space? Cyber space refers to the virtual connections which occur due to Internet and through which we can visit various virtual locations (websites and web portals) for both work/services and entertainment1. It is important that such website or web portals that a computer user visits, does not make him/her vulnerable to cyber attacks [3]. The onus of making this cyber space safe is not dependent on only the computer user or the ISP (Internet service providers) but also the government. Thus cyber security is an implementation which has a layered architecture.

We can say that Cyber security actually is a 3 dimensional architecture and requires implementation in each of the 3 views separately. These views may be elaborated as follows:

- Cyber Policies View
- Infrastructure View
- Software Process View

The above can be better understood via Figure No. 1 as given below:

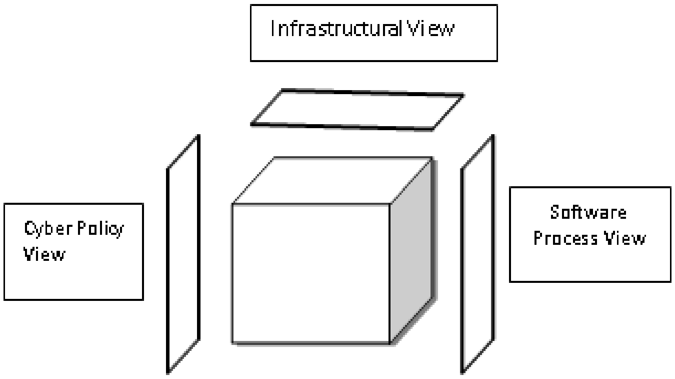


Figure 1: 3-Dimensional View of Cyber Security Implementation

2. CYBER POLICY VIEW

This view focuses on the requirement of government setting up policies through which cyber security defenses can be set up. These may be elaborated into following classes [2]:

2.1. Building Analytical Process for Monitoring Cyber Attack

This is the first line of action when building cyber security policy. It requires the organization to build a Data repository containing extensive datasets of cyber-attacks from known compromised sources. This dataset may then be studied and updated with new cyber-attacks so as to build effective anti-cyber-attack walls.

2.2. Standardization of Measurement Metrics for Various Security Measures

This is the second line of action while building policies to safe guard against cyber terrorism. This not only requires the people at all government and ISP level to use same security names and parameters but also requires all governmental and nongovernmental organizations to cooperate with each other and concur for common and effective metrics for measurement of various security measures so that in terms of emergency security and safety measures may be implemented smoothly and without hassle.

2.3. Hierarchical Structure Through Risk Prioritization

This is important factor for controlling risk. It may be realized in a hierarchical structure by implementing following parameters:

- Exclusion
- Replacement
- Seclusion
- Security Controls
- Administrative Parametric Control
- Personal Security Protective Gear

2.4. Continuous Up gradation of Security Parameters

Indian authorities must hold International symposiums and conferences where experts from various countries must come together to deliberate upon up gradations that must be done for various security parameters depending upon the flow of cyber crime at that movement.

2.5. Cyber Defense Automation

Dream of 'Digital India' also requires a large budget to be set aside for the full automation of various security controls in a layered format so that breaking into the whole network becomes almost next to impossible. This would require strategizing the defenses and automating them through the use of various software e.g. SIEM, firewalls etc.

3. INFRASTRUCTURAL VIEW

This view of the 3Dimensional architecture of Cyber Security pays detailed attention to the hardware aspect of the network. Guidelines framed in the First dimension must now take physical shape. This may be achieved by following points:

3.1. Building a list of sanctioned and illegal equipments within Government departments and crucial Banking as well as Telecom Networks [4]

Since Government and bank data is the most sought after during a cyber attack the first line of defense against it must be to build and enforce a list of authorized and unauthorized equipments that may be connected to the networks of these targets. This will act like an insurance policy against cyber attack and will reduce the chance of success of such a threat to a large extent.

3.2. Building a list of sanctioned and illegal equipments within Government departments and crucial Banking as well as Telecom Networks

Not only is it important to have a list of sanctioned and unsanctioned devices, it is also important to create a sanctioned and unsanctioned list of software which can be used in these crucial data banks so that cyber threat can be deterred.

3.3. Assiduous vulnerability Estimation & Improvement

All networks and their equipments must be weekly scanned by cyber susceptibility management tools so as to identify any and all cyber breaches. It is also required to update all software systems and install operating system patches so that no weak points are left which may be exploited by the hackers.

3.4. Preserve and Scrutinize Audit Logs

All records such as log files of network and network equipments and there software must be properly stored and scrutinized for prevention and recovery from cyber attacks.

3.5. Data Recovery and Backup

Another very important requirement of a secure network is to have a Specialized Data Recovery and Backup unit for all Government, Banks, Healthcare and Telecom networks so that when a cyber attack takes place, the recovery process from it is smooth and fast.

3.6. Secure Network and Device hardware and software configurations

It is also important that all network configurations such as firewalls settings; router configurations etc must be done as per set standards and recorded properly. It is also important to have Malware protection and proper Email and Web Browser protection in place against cyber attacks.

4. SOFTWARE PROCESS VIEW

The third and the most important view of 3D Cyber Security Architecture is the Software Process View. This view is composed of minimum 3 components which may be listed as follows [6] :

4.1. Component One: Automatic Threat Identification through Machine Learning Algorithms such as MLP

MLP or Multilayered Perceptron is an Artificial Neural Network (ANN) technique through which classification of data can take place. It is a supervised learning tool that learns a function by training on a dataset and gives an optimum regression output. A MLP has a 3 layered architecture.

Input layer is the first layer of MLP. It takes in input data which then is passed onto second layer of MLP which is called the hidden layer. The last layer of MLP is called the Output Layer. In our paper we took 45 important network parameters and trained our MLP using them. The result of regression can be seen in figure 3.

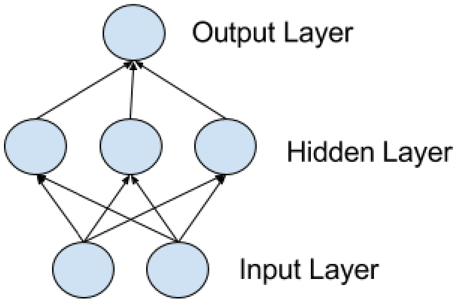


Figure 2 - Three Layered Neuron

The below regression chart shows that through machine learning we can easily identify as well as correctly classify our input dataset into different types of cyber attacks in a very short period of time and thus take corrective actions. Successful result on a dataset of 1000 entries was successfully achieved in a mere 17.36 Seconds. It may be inferred that such Machine learning techniques must be made as first line of defense in cyber security.

4.2. Component Two: Sentiment Analysis [5]

Since its successful implementation in data analytics, much stress has been laid on the use of Sentiment Analytics in the field of Cyber Security. Sentiment Analytics involves opinion mining which involves analysis of sentiments, feelings, opinions, emotions and attitude.

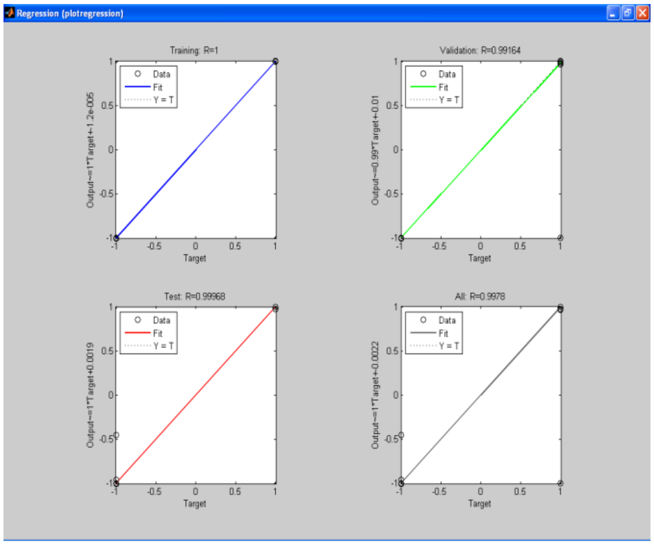
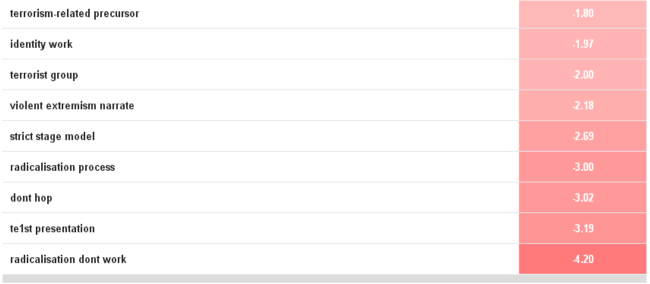


Figure 3- Regression analysis using Matlab for cyber security automation

There are various sentiment analysis algorithms which can be beneficial to tracking any clues of impending cyber security incident by crawling through various social media sites and gathering intelligence. The utilization of sentiment analysis can be understood more clearly through following example:

If we copy and paste the following URL ‘https://twitter.com/CTP_Swansea’ in a simple sentiment analysis process the output table of sentiments that we are able to gather can be seen in Figure no 4:



terrorism-related precursor	-1.80
identity work	-1.97
terrorist group	-2.00
violent extremism narrate	-2.18
strict stage model	-2.69
radicalisation process	-3.00
dont hop	-3.02
te1st presentation	-3.19
radicalisation dont work	-4.20

Fig 4: Sentiment Analysis on twitter handle regarding cyber security

5. SUMMARY

Digital India and strong cyber security arrangements are two concepts that can not exist without each other. Cyber security is better understood by a 3 Dimensional Architecture where all the three views play important role. Deep learning through MLP and sentiment analysis are techniques which can give Digital India initiative unmatched backup in an event of tragedy and thus must be incorporated in Digital India dream of a smooth and corruption free society.

6. CONCLUSION

Conclusion part depicts the main points as the constructive finds obtained from the proposed system. Conclusion should not be the same as abstract. Conclusion should be modeled efficiently.

REFERENCES

[1] GOSWAMI, Himakshi. Opportunities And Challenges Of Digital India Programme. International Education and Research Journal, [S.l.], v. 2, n. 11, nov. 2016. ISSN 2454-9916. Available at: <http://ierj.in/journal/index.php/ierj/article/view/541>.

[2] Dr. Goutam Chakraborty and Murali Krishna Pagolu, “Analysis of Unstructured Data: Applications of Text Analytics and Sentiment Mining”, SAS GLOBALFORUM PROCEEDINGS, 2014

[3] http://www.thehindubusinessline.com/money-and-banking/mobile-apps-of-7-indian-banks-compromised-fireeye/article9618128.ece.

[4] Robert M. Lee, “The sliding scale of cyber security”, A SANS Analyst paper”, August 2015.

[5] Apoorv Agarwal, Boyi Xie Ilia, Vovsha Owen Rambow , Rebecca Passonneau, “Sentiment Analysis of Twitter Data”, Dept. of Computer Science, Columbia University, New York, USA.

[6] Agam Das Goswami, M. K. Mishra, Dipti Patra, “Investigation of general regression neural network architecture for grade estimation of an Indian iron ore deposit”, Arabian Journal of Geosciences, Feb 2017.