# Cyber Security Monitoring in India by Probability Calculation

**Priyanka Kushwaha[1] Deepak Agrawal[2]**
[1,2]Department of Computer Science & Engineering
[1,2]Takshshila Institute of Engineering & Technology, Jabalpur MP, India

*Abstract*— The 'security sensitivity' is unlikely to alter through enhancements to usability alone rather; angle changes need future social amendment. Yet, to date, very little theoretical add usable privacy and security has applied science theory to know however social processes have an effect on security sensitivity. In turn, this lack of theoretical insight has precluded systems work that accounts for the social consequences of security system style. Thus, there remains an excellent however for the most part untapped chance to model human social behaviours among the context of cyber security and in making socially intelligent security systems that have an improved understanding of those human social behaviours. To bridge these gaps in theory and observe, during this thesis, I supply Associate in adversary initial theory of however social influences have an effect on cyber security behaviours, distil these theoretical insights into a group of broad style recommendations, so implement and appraise to such systems that time to a way forward for social intelligent cyber security.

***Key words:*** Cyber Security, Security Sensitivity, Cyber Security Behaviors

## I. INTRODUCTION

As India is finance heavily in building e-services for its voters by providing higher bandwidths and integration economic system with digital marketplace, there's associate degree augmented would like for stress on cyber security in Asian nation. The cyber security threats or Cyber-attacks usually emanate from a spread of sources and manifest themselves in riotous activities that concentrate on people, businesses, national infrastructure, business institutions and Governments alike. Therefore, cyber security is seen because the latest tenant of the safety challenge since major important infrastructure as well as, banking, defense, power, etc. square measure shifting to the digital realm. The consequences of a vulnerable cyber house carry important risk for public safety, national security and stability of the globally joined economy. Hence, cyber security threats because a significant economic and national security challenge for our country in present times [5].

The seriousness of this downside is highlighted after you think about that future technologies can enable extraordinarily necessary identifiers, similar to a retinal scan or a fingerprint, to be drawn digitally. These biometry characteristics square measure protected in real house as a result of their embedded within the material body of the person. This is lost in cyberspace. Thus, computer network wants a system that enables people to verify their identities to others while not revealing to them the digital illustration of their identities. [3]

## II. CYBER SECURITY PREPARATION OF INDIA

The initiatives taken by the govt. of Asian nation have centered on threats to important info infrastructure and national security, adoption of relevant security technologies, info security awareness, coaching and analysis. Thanks to dynamic nature of cyber threat situation, these actions have to be compelled to be continuing, refined and strong from time to time. There have been some steps taken:

1) The Information Technology (Amendment) Act 2008 has been enacted to cater to the requirements of National Cyber Security.
2) Indian Computer Emergency Response Team (CERT-In) has been operational as a national agency for cyber security incident response.
3) Growth and application of digital signature certificates during a range of areas has taken place.
4) National Crisis Management arranges for countering cyber-attacks and cyber coercion has been ready and is annually updated.
5) The Information Technology (Amendment) Act 2000 has been enacted to cater to the requirements of National Cyber Security.
6) Indian Computer Emergency Response Team (CERT-In) has been operational as a national agency for cyber security incident response.
7) The CERT- In (Computer Emergency Response Team) is terribly undermanned to manage the coverage rise in cybercrimes. From 22,000 reportable incidents in 2012, it's gone up to one.3 100000 cyber-attacks as reportable in 2014.
8) The National Cyber Security Policy came up in 2013 that has well ordered out fourteen parameters however the implementation has to be much stricter.
9) An organization presupposed to return up since 2014 National Cyber Coordination Centre however not abundant has been achieved during this space nevertheless.
10) National Crisis Management arranges for countering cyber-attacks and cyber coercion has been ready and is annually updated.

Growth and application of digital signature certificates during a range of areas has taken place. Security Auditors are empaneled for conducting security audits. Threats from hacker teams from hostile countries have been increasing day by day. The capacities developed to handle these cyber-attacks have to be compelled to be scaled up exponentially to affect the cyber risks Asian nation goes to face. NASSCOM has projected India would wish one million cyber security specialists by 2020 [2, 9]. Laisison with personal sector relating to cyber security incidents.

A Digital Signature could be a technique by that it's attainable to secure electronic info in such the simplest way that the conceiver of the data, similarly because the integrity of the data, may be verified. This procedure of guaranteeing the origin and also the integrity of the data is additionally referred to as Authentication [9]. The believability of the many legal, financial, and different documents is set by the presence or absence of a certified written signature. For a processed message system to switch the physical transport of

 

paper and ink documents written signatures ought to get replaced by Digital Signatures.

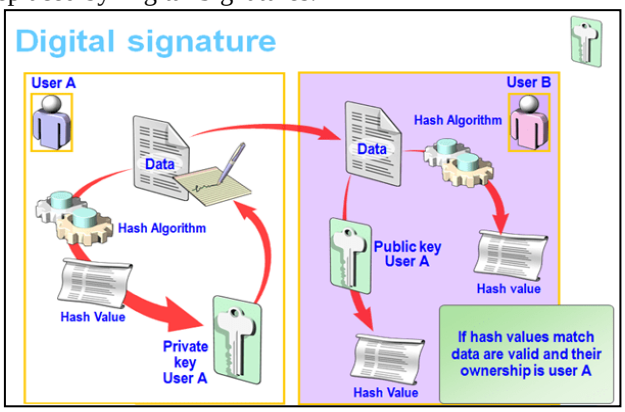


Fig. 1: Typical Digital Signature

## III. PROPOSED WORK

Government has many authority companies who monitor or control the activities of all the web links or applications provided by the internet. They also provide the feedback form to each of the customer who uses these web links or applications. Suppose there are 5 stars for giving the feedback [4]. Let, there are 3 probabilities Probability P represents the number of users who like the web or application for their desired purpose. It means they are satisfied. It also means that it is the Probability that these customers willing to again use those web links or applications in future.

Probability Q represents the number of users who unlike the web or application for their desired purpose. It means they are not satisfied. It also means that it is the Probability that these customers willing to never use those web links or applications in future.

Probability R represents the number of users who are neutral for giving the feedback to the web or application. Hence they are not serious for those web links or applications. This probability may be varying.

Now we calculate these three probabilities. For this purpose, in each of 29 states we selected 10 cities and monitor probabilities P (feedback as Star 4 or 5) & Q (feedback as unlike or unsubscribe). We monitor the percentage of users in each of the city in each of the states. Here we ignore less than 30% of users of probability P and Q.

| S. Name | S. No. | Percentage of Users | Probabilities (P) |
|---|---|---|---|
| Andhra Pradesh | 1 | 70, 80, 83, 85, 86, 88, 90 | 7 |
| Arunachal Pradesh | 2 | 71, 25, 58, 87, 65, 56, 85, 52 | 8 |
| Assam | 3 | 60, 70, 85, 59, 63, 32 | 6 |
| Bihar | 4 | 70, 80, 83, 85, 86, 88, 91, 93, 89, 90 | 10 |
| Chhattisgarh | 5 | 81, 65, 75, 62, 40 | 5 |
| Goa | 6 | 90, 74, 58, 80, 49, 8, 65 | 7 |
| Gujarat | 7 | 87, 48 | 2 |
| Haryana | 8 | 57, 61, 68, 61, 76 | 5 |
| Himachal Pradesh | 9 | 36, 98, 89, 33 | 4 |
| Jammu and Kashmir | 10 | 76 | 1 |
| Jharkhand | 11 | 95, 37 | 2 |
| Karnataka | 12 | 35, 45, 41 | 3 |
| Kerala | 13 | 92, 35, 98, 54, 61 | 5 |
| Madhya Pradesh | 14 | 74, 98, 31, 83, 57, 84, 76, 68 | 8 |
| Maharashtra | 15 | 61, 85, 65, 52, 90, 36, 98, 89, 43 | 9 |
| Manipur | 16 | 81, 75, 57, 52 | 4 |
| Meghalaya | 17 | 80, 84, 98, 30, 39, 48 | 6 |
| Mizoram | 18 | 88, 91, 80, 89, 90, 80, 83, 85, 86, 88 | 10 |
| Nagaland | 19 | 85, 37, 76, 98, 31, 83, 57, 84, 76 | 9 |
| Odisha | 20 | 71, 35, 58, 87, 65, 56, 45, 62 | 8 |
| Punjab | 21 | 42, 85, 32, 82, 58, 58, 46, 53, 92 | 9 |
| Rajasthan | 22 | 75, 48, 42, 77, 76 | 5 |
| Sikkim | 23 | 61, 55, 93, 52, 54, 86 | 6 |
| Tamil Nadu | 24 | 78, 62 | 2 |
| Telangana | 25 | 55, 56, 32, 65, 45, 67, 82 | 7 |
| Tripura | 26 | 81, 55 | 2 |
| Uttar Pradesh | 27 | 62, 32, 88, 34, 80, 66, 69, 83, 81 | 9 |
| Uttarakhand | 28 | 88, 65, 33 | 3 |
| West Bengal | 29 | 45, 54, 75, 32 | 4 |

Table 1: 29 States We Selected 10 Cities & Monitor Probabilities P (Feedback as Star 4 Or 5)

| S. Name | S. No. | Values | Probabilities (Q) |
|---|---|---|---|
| Andhra Pradesh | 1 | 75, 83 | 2 |
| Arunachal Pradesh | 2 | 78 | 1 |
| Assam | 3 | 55, 45, 67, 82, 82 | 5 |
| Bihar | 4 | 59 | 1 |
| Chhattisgarh | 5 | 62, 32, 90, 34, 78, 45, 65, 28, 21 | 9 |
| Goa | 6 | 86, 65, 34, 86 | 4 |
| Gujarat | 7 | 45, 54, 75, 32, 85, 79, 65, 32 | 8 |
| Haryana | 8 | 86 | 1 |
| Himachal Pradesh | 9 | 32, 30, 75, 68, 84, 53, 45, 58, 96 | 9 |
| Jammu and Kashmir | 10 | 52, 73 | 2 |
| Jharkhand | 11 | 54, 30, 38 | 3 |
| Karnataka | 12 | 78, 45, 53 | 3 |
| Kerala | 13 | 32, 48, 39, 32, 79, 65, 32 | 7 |
| Madhya Pradesh | 14 | 75, 48, 42, 77, 38, 78, 65 | 7 |
| Maharashtra | 15 | 70, 80, 83, 85, 86, 88, 90, 85 | 8 |
| Manipur | 16 | 51, 55, 50, 72, 78, 76, 38, 25 | 8 |
| Meghalaya | 17 | 70, 84, 68, 62 | 4 |
| Mizoram | 18 | 88, 96 | 2 |
| Nagaland | 19 | 49 | 1 |
| Odisha | 20 | 71, 85, 58 | 3 |
| Punjab | 21 | 42, 75, 78, 86, 36, 35, 32, 48 | 8 |
| Rajasthan | 22 | 75, 48, 42, 77, 66, 78, 53, 69, 25 | 9 |
| Sikkim | 23 | 84 | 1 |
| Tamil Nadu | 24 | 76 | 1 |
| Telangana | 25 | 52, 56, 32, 85 | 4 |
| Tripura | 26 | 71, 85, 35, 86, 81, 39 | 6 |
| Uttar Pradesh | 27 | 99, 90, 85, 66 | 4 |
| Uttarakhand | 28 | 78, 45, 53, 37, 73, 50, 83 | 7 |
| West Bengal | 29 | 32, 48, 39, 58, 32, 78 | 6 |

Table 2: 29 States We Selected 10 Cities & Monitor Probabilities Q (Feedback as Unlike or Unsubscribe)

We know that

$$P + Q + R = 1 \ldots\ldots\ldots\ldots \quad (1)$$

Therefore probabilities are divided by 1000 in order to satisfy equation (1).

$$0.17 + 0.13 + R = 1$$

Now R = 1 – 0.17 – 0.13
R = 1 – 0.30
R = 0.70

Probability of R represents the number of users who are neutral for giving the feedback to the web or application. It should be low. They need to be educated about the Cyber Security. Now we calculate the average of the information given by the users in the form of feedback. It is known as Entropy. A monitoring system not only dealing with a single city but with all the cities, hence the feedback may be described in average probability per individual city, called Entropy.

Let M= total number of cities

Then entropy for P is-

$$\text{Like}_{\text{avg}} = \text{Entropy} = -\sum_{k=1}^{M} \frac{1}{P}.\log_2 \frac{1}{P} \text{ Like / City}$$

| Proabability (PK) | | | log(Pk) | PK * log(Pk) |
|---|---|---|---|---|
| Andhra Pradesh | 7 | 0.007 | 2.15 | 0.02 |
| Arunachal Pradesh | 8 | 0.008 | 2.10 | 0.02 |
| Assam | 6 | 0.006 | 2.22 | 0.01 |
| Bihar | 10 | 0.01 | 2.00 | 0.02 |
| Chhattisgarh | 5 | 0.005 | 2.30 | 0.01 |
| Goa | 7 | 0.007 | 2.15 | 0.02 |
| Gujarat | 2 | 0.002 | 2.70 | 0.01 |
| Haryana | 5 | 0.005 | 2.30 | 0.01 |
| Himachal Pradesh | 4 | 0.004 | 2.40 | 0.01 |
| Jammu and Kashmir | 1 | 0.001 | 3.00 | 0.00 |
| Jharkhand | 2 | 0.002 | 2.70 | 0.01 |
| Karnataka | 3 | 0.003 | 2.52 | 0.01 |
| Kerala | 5 | 0.005 | 2.30 | 0.01 |
| Madhya Pradesh | 8 | 0.008 | 2.10 | 0.02 |
| Maharashtra | 9 | 0.009 | 2.05 | 0.02 |
| Manipur | 4 | 0.004 | 2.40 | 0.01 |
| Meghalaya | 6 | 0.006 | 2.22 | 0.01 |
| Mizoram | 10 | 0.01 | 2.00 | 0.02 |
| Nagaland | 9 | 0.009 | 2.05 | 0.02 |
| Odisha | 8 | 0.008 | 2.10 | 0.02 |
| Punjab | 9 | 0.009 | 2.05 | 0.02 |
| Rajasthan | 5 | 0.005 | 2.30 | 0.01 |
| Sikkim | 6 | 0.006 | 2.22 | 0.01 |
| Tamil Nadu | 2 | 0.002 | 2.70 | 0.01 |
| Telangana | 7 | 0.007 | 2.15 | 0.02 |
| Tripura | 2 | 0.002 | 2.70 | 0.01 |
| Uttar Pradesh | 9 | 0.009 | 2.05 | 0.02 |
| Uttarakhand | 3 | 0.003 | 2.52 | 0.01 |
| West Bengal | 4 | 0.004 | 2.40 | 0.01 |
| P = 0.17 | | | Entropy = P * log(P) 0.3637 | |

Table 3: Entropy calculation for P (Feedback as Star 4 or 5)

$\text{Like}_{\text{avg}} = \text{Entropy} = 0.3637$ Like / City

To compensate it should be multiplied by 1000.

$\text{Like}_{\text{avg}} = \text{Entropy} = 0.3637 \text{ X } 1000$ Like / City

$\text{Like}_{\text{avg}} = \text{Entropy} = 363.7$ Like / City

| Proabability (QK) | | | log(Qk) | QK * log(Qk) |
|---|---|---|---|---|
| Andhra Pradesh | 2 | 0.002 | 2.70 | 0.01 |
| Arunachal Pradesh | 1 | 0.001 | 3.00 | 0.00 |
| Assam | 5 | 0.005 | 2.30 | 0.01 |
| Bihar | 1 | 0.001 | 3.00 | 0.00 |
| Chhattisgarh | 9 | 0.009 | 2.05 | 0.02 |
| Goa | 4 | 0.004 | 2.40 | 0.01 |
| Gujarat | 8 | 0.008 | 2.10 | 0.02 |
| Haryana | 1 | 0.001 | 3.00 | 0.00 |
| Himachal Pradesh | 9 | 0.009 | 2.05 | 0.02 |
| Jammu and Kashmir | 2 | 0.002 | 2.70 | 0.01 |
| Jharkhand | 3 | 0.003 | 2.52 | 0.01 |
| Karnataka | 3 | 0.003 | 2.52 | 0.01 |
| Kerala | 7 | 0.007 | 2.15 | 0.02 |
| Madhya Pradesh | 7 | 0.007 | 2.15 | 0.02 |
| Maharashtra | 8 | 0.008 | 2.10 | 0.02 |
| Manipur | 8 | 0.008 | 2.10 | 0.02 |
| Meghalaya | 4 | 0.004 | 2.40 | 0.01 |
| Mizoram | 2 | 0.002 | 2.70 | 0.01 |
| Nagaland | 1 | 0.001 | 3.00 | 0.00 |
| Odisha | 3 | 0.003 | 2.52 | 0.01 |
| Punjab | 8 | 0.008 | 2.10 | 0.02 |
| Rajasthan | 9 | 0.009 | 2.05 | 0.02 |
| Sikkim | 1 | 0.001 | 3.00 | 0.00 |
| Tamil Nadu | 1 | 0.001 | 3.00 | 0.00 |
| Telangana | 4 | 0.004 | 2.40 | 0.01 |
| Tripura | 6 | 0.006 | 2.22 | 0.01 |
| Uttar Pradesh | 4 | 0.004 | 2.40 | 0.01 |
| Uttarakhand | 7 | 0.007 | 2.15 | 0.02 |
| West Bengal | 6 | 0.006 | 2.22 | 0.01 |
| Q = 0.13 | | | Entropy = Q * log(Q) 0.3010 | |

Table 4: Entropy calculation for Q (Feedback as unlike or unsubscribe)

Similarly entropy for Q is-

$$\text{Unlike}_{\text{avg}} = \text{Entropy} = -\sum_{k=1}^{M} \frac{1}{Q}.\log_2 \frac{1}{Q} \text{ Like / City}$$

$\text{Unlike}_{\text{avg}} = \text{Entropy} = 0.3010$ Unlike / City

To compensate it should be multiplied by 1000.

$\text{Unlike}_{\text{avg}} = \text{Entropy} = 0.3010 \text{ X } 1000$ Unlike / City

$\text{Unlike}_{\text{avg}} = \text{Entropy} = 301.0$ Unlike / City

– Results

1) P = 0.17
2) Q = 0.13
3) R = 0.70
4) $\text{Like}_{\text{avg}} = \text{Entropy} = 363.7$ Like / City
5) $\text{Unlike}_{\text{avg}} = \text{Entropy} = 301.0$ Unlike / City

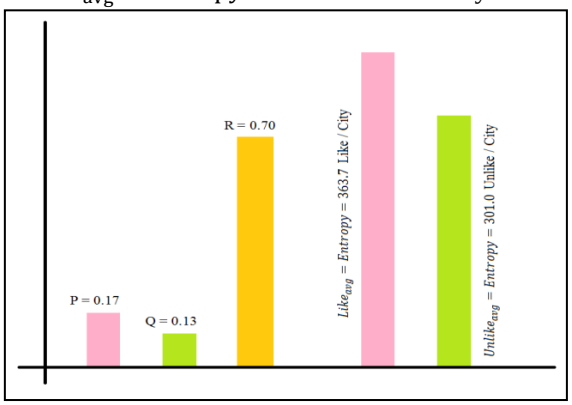


Fig. 2:

## IV. CONCLUSIONS & FUTURE WORKS

From the results following observations are done.

1) Entropy of P represents the number of users who like the web or application for their desired purpose. It means they are satisfied. If it is higher; then the service should be granted for future.

2) Entropy of Q represents the number of users who unlike the web or application for their desired purpose. It means they are not satisfied. If it is higher; then the service should be denied for future.
3) Probability of R represents the number of users who are neutral for giving the feedback to the web or application. This rate should be low. They need to be educated for the Cyber Security.

These observations will be helpful for the govt. Authorities to predict on the cyber security. Because the general population becomes increasingly progressively more and a lot of refined in their understanding and use of computers and because the technologies related to computing become more powerful, there's a robust chance that cybercrimes can become a lot of common. India is rated collectively of the countries with the very best levels of e-crime activities. Cyber security should be self-addressed seriously because it affects the image of the country within the outside the planet. A mixture of sound technical measures tailored to the origin of Spam (the causing ends) in conjunction with legal deterrents are going to be a decent begins within the war against cyber criminals. Data attacks are launched by anyone, from any place. The attackers will operate while not detection for years and may stay hidden from any counter measures. This so emphasizes the requirement for the govt. security agencies to notice that there ought to carry on with technological and security advancements. It'll invariably be a losing battle if security professionals square measure miles behind the cyber criminals. Fighting law breaking needs a holistic approach to combat these menace altogether ramifications. There ought to produce a security-aware culture involving the general public, the ISPs, cybercafés, government, security agencies and web users. Conjointly in terms of strategy, it's crucial to totally address problems regarding social control. Mishandling of social control will backfire. How will we tend to smart and intelligent systems that encourage higher cyber security behaviors? It is a most challenging goal in front of Indian Government.

## REFERENCES

[1] Alpna and Dr. Sona Malhotra, " Cyber Crime-Its Types, Analysis and Prevention Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 5, May 2016 ISSN: 2277 128X.
[2] Dr. Ajeet Singh Poonia, "Cyber Crime: Challenges and its Classification", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) , Volume 3, Issue 6, November-December 2014 ISSN 2278-6856.
[3] Atul M. Tonge, Suraj S. Kasture and Surbhi R. Chaudhari, "Cyber security: challenges for society-literature review", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 12, Issue 2 (May. - Jun. 2013), PP 67-75.
[4] Dr. Jünger Albinger (PhD), "Business Intelligence Journal", Business Intelligence Journal January, 2010 Vol.3 No.1, Volume 3 - Number 1 Published by the IIU Press and Research Centre, Belgium, for the Department of Business Management and Economics (BME) of the School of Doctoral Studies (European Union).
[5] Ajeet Singh Poonia, Dr. Awadesh Bhardwaj and Dr. G. S. Dangayach, "Cyber Crime: Practices and Policies for Its Prevention", the First International Conference on Interdisciplinary Research and Development, 31 May - 1 June 2011, Thailand.
[6] Vaishnav Mruga Bhadreshbhai, Prajapati Nikita Dineshbhai and MR. Piyush Patel, "Growing Cybercrimes in India: A Survey", IJIRST, National Conference on Latest Trends in Networking and Cyber Security, March 2017.
[7] Dr. Mike McGuire and Samantha Dowling, "Cybercrime: A review of the evidence Research Report 75", Home Office, and October 2013.
[8] M. Elavarasi and N. M. Elango, "Analysis of Cybercrime Investigation Mechanism in India", Indian Journal of Science and Technology, Vol 10(40), DOI: 10.17485/ijst/2017/v10i40/119416, October 2017 ISSN (Print): 0974-6846 ISSN (Online): 0974-5645.
[9] Priya Singh, Neeraj Saini and Rajkumar Saini, "Cyber Crime and its Related Aspects under I.T. Act, 2000 and its Prevention", International Journal of Computer Applications (0975 – 8887) Volume 127 – No.16, October 2015.
[10] Vineet Kandpal and R. K. Singh, "Latest Face of Cybercrime and Its Prevention in India", International Journal of Basic and Applied Sciences Vol. 2. No- 4, 2013, Pp. 150-156, ISSN: 2277-1921.

 