An IT-Empirical Defusion of Online Offline Fake Government of Telangana (OOFGoT)

N.Srihari Rao,

Research Scholar, JNTUA, Anantapuramu,

K.Chandra Sekharaiah,

Professor in SIT, JNTUH, Hyderabad,

A.Ananda Rao,

Director R&D, JNTUA, Anantapuramu,

Abstract

Currently, in India and worldwide, the number of cybercrime cases is rapidly increasing, as can be seen in different types of social media such as news groups on the Internet, online news sites, most popular news papers, and magazines we really depend on for latest news. Cybercrime is the crime committed using computer as a tool or a target. We have taken up a cybercrime case study related to JNTUHJAC and Fake Government of Telangana (FGoT) cybercriminal organization, as part of our research work, and have been tracking the progression and response against these cybercrimes by the related public authorities namely, JNTUH University administrators, and police personnel of K.P.H.B Police Station, Hyderabad. The two organizations namely i) http://jntuhjac.com which is an online organization with the cybercriminal content in the image to the R.H.S of its home page is known as Online Fake Government of Telangana (Online FGoT) and ii) JNTUHJAC which is an offline organization, prevalent in the academic premises of the JNTUH academic community continuing its organized activities, is known as Offline Fake Government of Telangana (Offline FGoT). These two organizations were born in 2011 and prevalent during the Telangana separatist movement in the years 2011-2014. They still exist in JNTUH academic community and are collectively known as the Online Offline Fake Government of Telangana (OOFGoT).

We utilized various types of IT devices to defuse the cybercriminal activities of OOFGoT such as ICT approaches, Social Networking Site accounts and Information Transparency principle. We also opted various empirical ways such as field reporting, forming Pronational workforce, and publishing well-indexed research papers etc. to defuse the effects of these cybercrimes. It is reflected through our research publications made over many years in our research group. We have brought out the Pronational workforce recently in 2018 year, which builds and develops Quality-of-National-Life (QoNL) and paves way to Road to Information Technology (RIT) by means of RTI. This way we contribute to the success of right Information Technology, i.e. RIT. We brought awareness about the context of this cybercrime among public authorities, and the response from the public authorities namely, Governor's Secretariat, the Prime Minister's Office, A.P Secretariat Office, Rajya Sabha Secretariat, TSPSC, and DST reflect the fact that these kinds of cybercrime incidents were not desirable for any nation. They destroy the national spirit and pave way for more cybercrimes, if the related cybercriminals are left unpunished. We gathered data through RTI Act 2005 from the above mentioned public authorities, and analyzed to bring out the essence and required methods for handling cyber crimes of related types. We sensitized and insisted proper cyberpolicing to pass prohibition orders against the JNTUHJAC and FGoT cybercrimnal organizations and to rightly work for conviction of these cybercriminals.

1. Introduction

Cybercrimes are crimes which are either targeted at computers/other devices as in hacking (computer is the target here), or crimes in which computers or other devices are integral to the offence as in online fraud, identity theft etc (computer is the tool here). The effect of cybercrime can be extremely upsetting for victims, and not necessarily just for financial reasons. Victims may feel that their privacy has been violated, and that they are powerless. Recently, in India efforts like demonetization, large scale digital economy extremely increased reliance on technology. Unfortunately, this extreme reliance on technology also increases the cost and incidence of cybercrime. As shown in figure 1(a) there are different varieties of cybercrimes that belong to any of the two types mentioned above. Cyber laws should safeguard the national fabric from cybercrimes.

The two cybercriminal organizations namely JNTUHJAC and FGoT were prevalent in JNTUH academic environment since 2011. The website with URL http://jntuhjac.com has been led by JNTUHJAC offline organization which has been prevalent from the year 2011 to till date in the JNTUH academic environment [1]. Through the web crawler tool, we captured some snapshots of the homepage of this website available between the dates from 12Nov2011 to 18Mar2014 [2] and found to have some cybercriminal content in its web pages. The image with a logo can be seen in figure 1(b) below that contains Indian National Emblem. The usage of the state emblem of India in a way that is prohibited by the 'State Emblem of India (Prohibition of Improper Use) Act, 2005 is a cybercrime perpetrated against India by an organized group known as JNTUHJAC that has association with FGoT and hence is a culprit group committing a cognizable crime.

(a)   (b)

Figure 1: a) Different Varieties of Cybercrimes

b) Cybercriminal Content in the Logo as on 12November2011

We also find mention of "Government of Telangana" in the logo on the R.H.S which is prejudiced to law and constitution of India during the years 2011, 2012, 2013 and in the first half of year 2014. The logo is part of the image during the years 2011-14. Figure 2 shows the screenshot of the homepage of the website with URL: http://jntuhjac.com as on 12November2011 extracted using Wayback machine's web crawler tool. After Mar2014, the culprit website removed the image with the above said logo. The organization JNTUHJAC was affiliated to the online Cheating Government of Telangana (CGoT) and the Seditious Government of Telangana (SGoT) [3]. This is a Fake Government of Telangana (FGoT) which has been operational in the JNTUH Hyderabad during 2011-14 and is misleading and cheating the nation. The cybercriminal impact is that the academic spirit got affected badly among the inmates of the JNTUH and the relevant crimes tend to affect badly the national amity, national spirit, national consciousness, national solidarity and national unity and integrity.

2. Online Offline Fake Government of Telangana (OOFGoT)

Online FGoT

http://jntuhjac.com is a website with the cybercriminal content in the image to the R.H.S of its home page is known as Online Fake Government of Telangana (Online-FGoT). It committed nearly four cybercrimes, namely 1. SEIPIUA violation, 2. Cheating the Nation crime, 3. Sedition Law violation, and 4. Identity Theft [4-6]. It is an organized online cybercriminal group with nearly 2014 members registered in it. It has more than 20,000 as the value for the degree of cybercrime.

Figure 2: Screenshot dated 12Nov2011

Not-online FGoT (Offline FGoT)

The JNTUHJAC which is an offline organized cybercriminal group has been prevailing in the JNTUH academic environment since 2011. There is a clear cut evidence collected and stored by us against the association of Online FGoT mentioned above with the JNTUHJAC. JNTUHJAC is an India abusive cybercrime group [26-27] as depicted in figure 3 below.

Figure 3: JNTUHJAC - an Offline Organization Prevalent in the JNTUH Academic Community is an Abusive Team

3. Research Methodology

Our research methodology comprises the steps and methodology that can be utilized effectively for the defusion of the deleterious impacts of the OOFGoT.

A. Online Offline Defusion of FGoT

Online and offline criminal activities of FGoT require both online and offline defusing mechanisms for effective remedy. The figure 4 shown below depicts how the online and offline defusion methods, Knowledge Management (KM), Knowledge Engineering (KE), and Data Collection and Analysis (DCA) systems are meant for defusing the deleterious effects of online offline criminal activities in the community or societal context. The online offline remedial activities greatly assist in transforming the ill-effected cybercriminal society into Swach Digital society [7-12]. Though we mentioned Knowledge Engineering

and Knowledge Management systems as remedial measures for cybercrimes, they are not the subject under detailed coverage in our work at present.
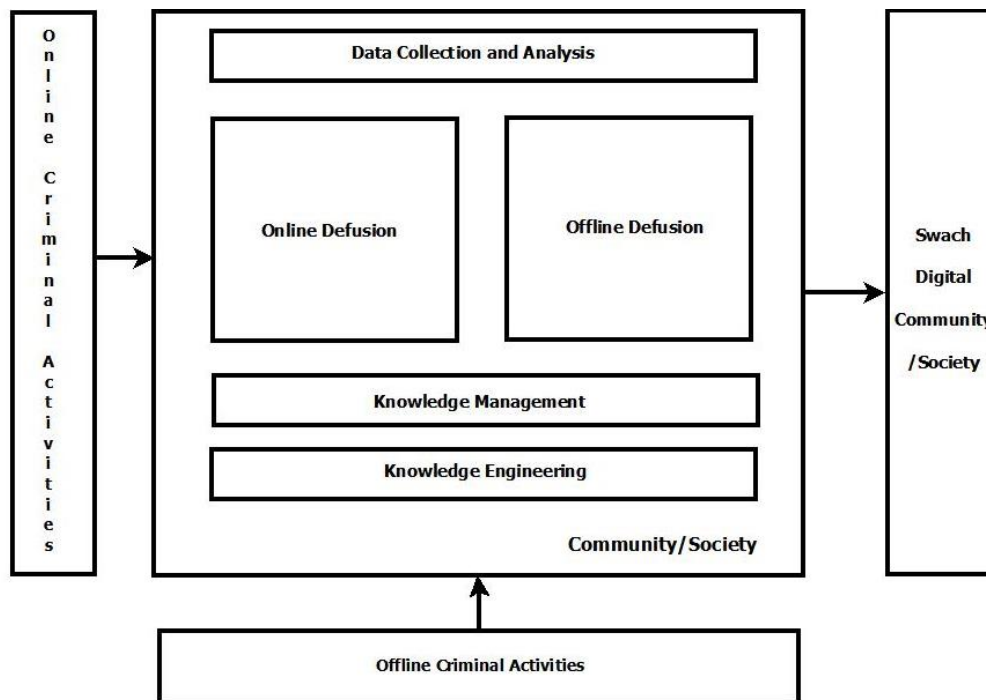

Figure 4: Online Offline Defusion of Deleterious Effects of Online Offline Fake Government of Telangana (OOFGoT)

Online Defusion of FGoT

Online defusion of FGoT refers to the activities that are conducted online such as guiding and bringing awareness to people through People's Governance Forum (PGF) web devices [13] as shown in figure 5, performing online social interactions with proper online communities on Internet for remedial analytics using Social Networking Site accounts such as Facebook, Twitter etc. as shown in figure 6 below. These activities drive the motivation for defusing the deleterious effects of the cybercrimes.
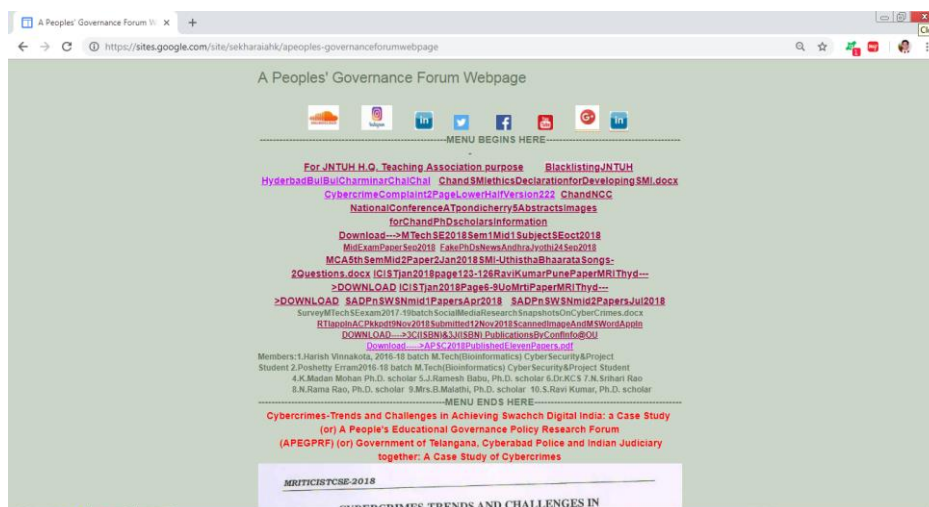
Figure 5: Snapshot of the People's Governance Forum(PGF) with URL:
https://sites.google.com/site/sekharaiahk/apeoples-governanceforumwebpage

Figure 6: Snapshot of the Facebook Account of Prof. K.Chandra Sekharaiah with URL: https://www.facebook.com/kcraiah showing interactions with peers and others

Not-online Defusion of FGoT

In our search of an exhaustive approach as the remedy of cybercrime, RTI Act 2005 was very much helpful as empirical tool and we have reasonably succeeded in our efforts as shown in figures 7(a) and 7(b). Forming Pronational workforce which works for the well being of our nation is itself another big achievement that has much empirical value [14-25].

(a)   **(b)**
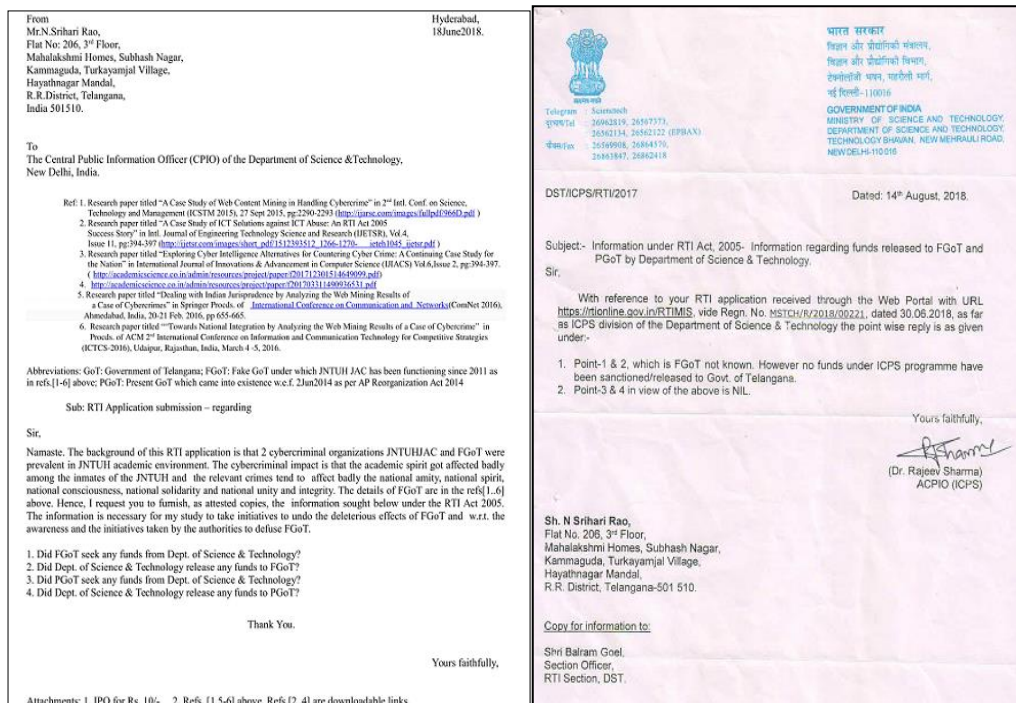
Figure 7: a) Image of the RTI Request Document Sent to Dept. of Science and Technology (DST), New Delhi b) Image of the RTI Response Document Received from DST, New Delhi

B. Data Collection and Analysis for Cybercrime Remedying

We gathered data through RTI Act 2005 from the public authorities mentioned in the table 1 below, and analyzed to bring out the essence and required methods for handling of these cybercrimes. We contributed significant time and efforts to bring awareness about these

cybercrimes to various supreme public authorities of our country. From the RTI requests sent and responses received by us, we empirically drew that the cybercrime case is effectively communicated to the above public authorities and their response indicates that the cybercrimes should be dealt properly. Otherwise, there will be an extreme increase in the cybercrime rate which endangers the nation and national spirit. We received the response from the PIO namely, Department of Science &Technology (DST) is as shown in figure 7(b) above. This sample indicates our efforts are fruitful and we have got the expected results.

Table1: Details of RTI Request-Response Communications with various Public Depts. of India

S.No	PIO Details	Response Received for RTI Request (Yes/No)	Responded with Proper Answers (Yes/No)	Usable for Data Analysis (Yes/No/ Partially)	First Appeal Sent in Case of no/Improper Response (Yes/No)	Response Received for Appeal (Yes/No)
1	**Principal Secretary to Governor**	Yes	No	Partially	Yes	Yes
2	**Principal Secretary to the Prime Minister**	Yes	No	Partially	Yes	No
3	**A.P Chief Secretary, A.P Secretariat Office**	Yes	Yes	Partially	Yes	No
4	**University Grants Commission (UGC)**	No	--	Partially	Yes	No
5	**Department of Science &Technology (DST)**	Yes	No	Partially	No	--
6	**Rajya Sabha Secretariat, Parliament House Annexe**	Yes	No	Partially	Yes	Yes
7	**Telangana State Public Service Commission (TSPSC)**	Yes	Yes	Yes	No	--

The figure 8 shown below is a tree that takes our efforts as mulch to nurture and produces the achievements as fruits of the tree to animal or human kind.
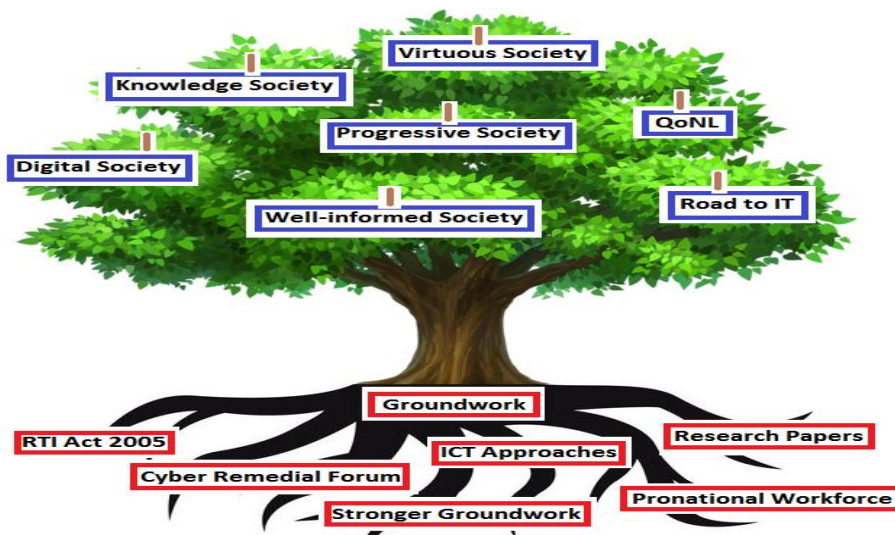

Figure 8: Tree of Efforts and Achievements

.

This research work was presented as a poster in Andhra Pradesh Science Congress-2018 conducted at Yogi Veamana University, Kadapa on 10November2018. That presentation was video recorded, uploaded in YouTube and can be found at URL: https://www.youtube.com/watch?v=beoe_zCrQzA.

5. Conclusions and Future Scope

We utilized both IT solutions and empirical studies for bringing out right information into JNTUH academic environment and hence into Telangana society. We brought awareness about the context of these cybercrimes among the close and concerned local public authorities through registration of complaints against these cybercrimes. We also gathered data through RTI applications from various supreme public authorities about their actions and reactions against these cybercrimes, and analyzed them for effective remedial analytics and handling of these cybercrimes. The response from these public authorities namely, Governor's Secretariat, the Prime Minister's Office, A.P Secretariat Office, DST, Rajya Sabha Secretariat, and TSPSC reflect the fact that these kinds of cybercrime incidents were not desirable for any nation. They destroy the national spirit and pave way for more cybercrimes, if the related cybercriminals are left unpunished. We sensitize and insist the cyberpolice to pass orders to prohibit the JNTUHJAC and FGoT cybercrimnal organizations and honestly work for conviction of these cybercriminals related to this cybercrime case [28-31]. We would work in future to bring out Knowledge-based systems and awareness systems and to set up systemic studies towards remedial solutions for any cybercrime.

References

[1] Usha Gayatri P., and Chandra Sekharaiah K., "Encasing the Baneful Side of Internet", National Conference on Computer Science & Security (COCSS 2013), 5-6 April 2013, Sardar Vallabhbhai Patel Institute of Technology, Vasad, Gujarat, India.

[2] B.Tirupathi Kumar , K.Chandra Sekharaiah , P.Mounitha, "A Case Study of Web Content Mining in Handling Cybercrime", International Journal of Advanced Research in Science & Engineering, Vol. No. 04, Special Issue (01), September 2015, www.ijarse.com ISSN 2319- 8354.

[3] P. Usha Gayatri, K Chandra Sekharaiah, D.Radhika, G.Sruthi, K.Satish, S.Mounika, K.Shravani, Ambuja Kulshreshtha, "Exploring Cyber Intelligence Alternatives for Countering Cyber Crime: A Continuing Case Study for the Nation", Proceedings of the Intnl Conf.@Bharati Vidyapeeth's Institute of Computer Applications and Management (BVICAM), New Delhi (INDIA).

[4] P. Usha Gayatri, K Chandra Sekharaiah, "A Case Study of Multiple Cybercrimes Against the Union of India", Presented in NCIST'2017@Manipur Institute of Technology, Manipur University & published in International Journal of Computer & Mathematical Sciences IJCMS ISSN 2347 – 8527 Volume 6, Issue 3 March 2017, pp.71-79.

[5] G.Aparna, P.Usha Gayatri, Seetha Mounika, D. Radhika, K Chandra Sekharaiah, "Reviewing a Judicial Case Study of Multiple Cybercrimes", in IndiaCOM2016 Intnl. Conf., BVICAM, New Delhi, Mar'16.

[6] P Usha Gayatri, K. Chandra Sekharaiah, P. premchand "Analytics of Judicial Case Study of Multiple Cyber Crimes against the Union of India" School of Law, Pondicherry University, Pondicherry, 2-3 March 2018.

[7] S Ravi Kumar, K Chandra Sekharaiah, Y.K Sundara Krishna, M Gouri Shenkar "Cybercrimes-Trends and Challenges in Achieving Swachch Digital India: a Case Study" MRITCISTCSE-2018, ISBN:97893 83038 596, Pg:6-8.

[8] S Ravi Kumar, K Chandra Sekharaiah, Y.K Sundara Krishna "Cybercrimes-Trends and Challenges in Achieving Swachch Digital India using a Public Cloud: A Case Study" School of Law, Pondicherry University, Pondicherry, 2-3 March 2018.

[9] Madan Mohan K., Chandra Sekharaiah K, A Case Study of ICT Solutions against ICT Abuse: An RTI Act 2005 Success Story, National Seminar on S&T for National Development, Manipur Univ., Imphal, Mar'17.

[10] N Srihari Rao, K Chandra Sekharaiah and A Ananda Rao" An Approach to Distinguish the Conditions of Flash Crowd versus DDoS Attacks and to remedy a Cyber Crime" School of Law, Pondicherry University, Pondicherry, 2-3 March 2018.

[11] N. Srihari Rao, K. ChandraSekharaiah & A. Ananda Rao,"An Approach to distinguish the conditions of Flash Crowd versus DDoS Attacks and to Remedy a Cyber Crime" in International Journal of Computer Engineering and Technology, 9(2), 2018, pp. 110-123.

[12] N.Srihari Rao, K.Chandra Sekharaiah, A.Ananda Rao. (2017) "A Survey of Distributed Denial of Service (DDoS) Defense Techniques in ISP Domains." In 5th International Conference on Innovations in Computer Science and Engineering (ICICSE-2017).

[13] https://sites.google.com/site/sekharaiahk/apeoples-governanceforumwebpage

[14] K Chandra Sekharaiah, "Impact of the RTI Act within a Public Authority Organization towards Employee-Employer Engagement: A Case Study", In proceedings of the Intnl. Conf., "ENRICHING EMPLOYEE ENGAGEMENT IN ORGANIZATION-ROLE OF PSYCHOLOGY", 30Jan-1Feb2015.

[15] K. Madan mohan, K Chandra Sekharaiah, P. Premchand "Impact of RTI Act with in Public Authority Organization Toward Employee Employer Engagement: A Case Study" School of Law, Pondicherry University, Pondicherry, 2-3 March 2018.

[16] Ramesh Babu J, Chandra Sekharaiah K, "Adaptive Management of Cybercriminal, Maladaptive Organizations, in the Offing, that Imperil the Nation" ICDMAI, Pune, 19-21 Jan 2018

[17] Ramesh Babu J, Chandra Sekharaiah K, "Adaptive Management of Cybercriminal, Maladaptive Organizations, in the Offing, that Imperil the Nation" IIT Kharaghpur, 2-3 March 2018.

[18] B. Tirupathi Kumar, K Chandra Sekharaiah, D. Suresh Babu "Towards National Integration by Analyzing the Web Mining Results of a Case of Cybercrime", in 2nd Intnl. Conf. on Information and Communication Technology for Competitive Strategies (ICTCS-2016) Udaipur, Rajasthan, India, 4-5Mar 2016.

[19] Gouri Shankar M. P.UshaGayatri, Niraja S., K Chandra Sekharaiah, "Dealing with Indian Jurisprudence by Analyzing the Web Mining Results of a Case of Cybercrimes", in Procds. of ComNet 2016 International Conference, 20-21 Feb. 2016, Ahmedabad, India.

[20] N. Srihari Rao, K. Chandra Sekharaiah, A. Ananda Rao, "Janani Janmabhoomischa Swargaadapi Gareeyasi", BVRIT, International Conference on Research Advancements in Applied Engineering Sciences, Computer and Communication Technologies, (ICRAAESCCT-18), 12-13Jul2018.

[21] N. Srihari Rao, K. Chandra Sekharaiah, A. Ananda Rao, "Janani Janmabhoomischa Swargaadapi Gareeyasi" International Journal of Engineering and Technology (IJET), Vol. 7,No. 3.29 (2018), pg. 225-231.

[22] K. Santhoshi, K. Chandra Sekharaiah, Naga lakshmi Kumari "ICT Based Social Policing for Swatch Digital India" School of Law, Pondicherry University, Pondicherry, 2-3 March 2018.

[23] N. Santhoshi, K. Chandra Sekharaiah, K. Madan Mohan, S. Ravi Kumar, B. Malathi, "Cyber intelligence Alternatives to Offset Online Sedition by in-Website Image Analysis through WebCrawler Cyber Forensics", in Procds. of International Conference on Soft Computing & Signal Processing (ICSCSP 2018) , June 22-23, 2018.

[24] K. Madan Mohan, K. Chandra Sekharaiah, N. Santhoshi, "ICT Approach to Defuse the Cybercriminal Sedition Dimension of Telangana Movement", BVRIT, International Conference on Research Advancements in Applied Engineering Sciences, Computer and Communication Technologies, (ICRAAESCCT-18), 12-13Jul2018.

[25] K. Madan Mohan, K.Chandra Sekharaiah, N.Santhoshi, "ICT Approach to Defuse the Cybercriminal Sedition Dimension of Telangana Movement", Accepted for publication in International Journal of Engineering and Technology (IJET), Vol. 7,No. 3.29 (2018).

[26] K.Pavana Johar, B.Malathi, S.Ravi Kumar, N.Srihari Rao, K.Madan Mohan, K.Chandra Sekharaiah, "India-abusive Government-of-Telangana (GoT2011): A Constitutional IT (an SMI) Solution", In Proceedings of International Conference on Science, Technology & Management (ICSTM-2018), Punjab University Campus, Chandigarh, India on 12th August 2018, ISBN: 978-93-87433-34-2.

[27] K.Pavana Johar, B.Malathi, S.Ravi Kumar, N.Srihari Rao, K.Madan Mohan, K.Chandra Sekharaiah, "India-abusive Government-of-Telangana (GoT2011): A Constitutional IT (an SMI) Solution", International Journal of Research in Electronics and Computer Engineering(IJRECE) Vol. 6 Issue 3 (July - September 2018) ISSN: 2393-9028 (PRINT) | ISSN: 2348-2281 (ONLINE), pp.1118-1124.

[28] N.Srihari Rao , J.Ramesh Babu, K.Madan Mohan, K.Pavana Johar, S.Ravi Kumar, K.Chandra Sekharaiah, A.Ananda Rao, "A Wolf in Sheep's Clothing- Fake Government of Telangana (FGoT), JNTUHJAC: Why 'not Prohibited?'", Proceedings of 3rd International Conference on Research Trends in Engineering, Applied Science and Management (ICRTESM-2018), Osmania University Centre for International Programmes, 4November 2018, pg.111-121, ISBN: 978-93-87433-44-1.

[29] N.Srihari Rao , J.Ramesh Babu, K.Madan Mohan, K.Pavana Johar, S.Ravi Kumar, K.Chandra Sekharaiah, A.Ananda Rao, "A Wolf in Sheep's Clothing- Fake Government of Telangana (FGoT), JNTUHJAC: Why 'not Prohibited?'", In International Journal of Management, Technology And Engineering(IJMTAE), Vol. 8, Issue XI, November2018, pp.532-542.

[30] K.Pavana Johar, M.Gouri Sankar, S.Ravi Kumar, K.Madan Mohan, P.Punitha, N.Santhoshi, B.Malathi, Ramesh Babu, N.Srihari Rao, K.Chandra Sekharaiah, "Cyberpolicing the Multifaceted Cybercriminal, Fake Government of Telangana : What is Sauce for the Goose is Sauce for the Gander", Proceedings of 3rd International Conference on Research Trends in Engineering, Applied Science and Management (ICRTESM-2018), Osmania University Centre for International Programmes, 4November 2018, pg.321-330, ISBN: 978-93-87433-44-1.

[31] K.Pavana Johar, M.Gouri Sankar, S.Ravi Kumar, K.Madan Mohan, P.Punitha, N.Santhoshi, B.Malathi, Ramesh Babu, N.Srihari Rao, K.Chandra Sekharaiah, "Cyberpolicing the Multifaceted Cybercriminal, Fake Government of Telangana : What is Sauce for the Goose is Sauce for the Gander", In Universal Review, Vol. 7, Issue XI, November2018, pp.256-264.