RESEARCH ARTICLE OPEN ACCESS

An Implementation of Search Engine Optimization Technique under Indian IT Law

Anuraj Singh [1], Jay Narayan Thakre [2], Dr. Taruna Jain [3]

MS Scholar [1], Assistant Professor [2]
Department of Information Technology
HOD Department of CSE [3]
Cyber Law & Information Security
University Institute of Technology –BU Bhopal
MP - India

ABSTRACT

Proposed work uses Search Engine Optimization (SEO) which permits the improvement of the position of a website on the search engines result pages. However, the practice of SEO is complex, and results are uncertain, because search engines do not communicate much about their ranking methods. Moreover, this activity takes time, and requires the implementation of modifications that can alter the visual effect and security level of the WebPages. In SEO search engine Security technique, the user illegally access information (wanted) & visits web site on which administrative officer keeps a record on weekly basis. In March 2017 the ideas developed on above platform as an experimental site. Once the idea is developed, the administrative officer keeps watch on the user who accesses the website and number of visits on approached website storing continues for three times. On first time access an alert is marked, on second time access on the same website high alert is marked, and third time access on the same website user is marked as Red alert. Administrative officer carry forwards all such Red alert SEO user data immediately to cyber forensic specialist team. Cyber forensic specialist team investigates the case and collects all evidences and decides about such user whether he is criminal or not and then applies Indian IT law under the Indian cyber law on the user.

Keywords: — SEO, Administrative offices role, Cyber Forensic specialist, Digital Evidence, Indian IT Law.

I. INTRODUCTION

Many people fail to take proper security measures when conducting research or storing their data. Conducting Search Engine Optimization (SEO) research requires a lot of patience and effort and can be a great deal of hard work. For above mentioned reason SEO data seems important and is increasingly valuable not only to a person and his organization but also to his competitors.

The strategically technique to take a web document of SEO user accessing data on a local SEO, observation or control by an administrative officer on an illegal activity or providing an authentication and maintaining a CIA Confidentiality at the same time, Integrity, Availability and keeping all record under SEO criminal Activity like URL web address, Access Time, Date, IP Address, MAC address for a top level security in Indian Domain comes under Indian IT law.

1.1 PROCESS OF SEO SECURITY TECHNIQUES

An overview and Analysis of Search engine optimization (SEO) Security techniques under Indian cyber Law as shown in Fig.1, may be demonstrated in following steps-.

- **User search information in SEO**
  SEO User search information as per personal requirement visit SEO and website by name and web address; SEO provide number of similar website, then user clicks a link of website and access information.

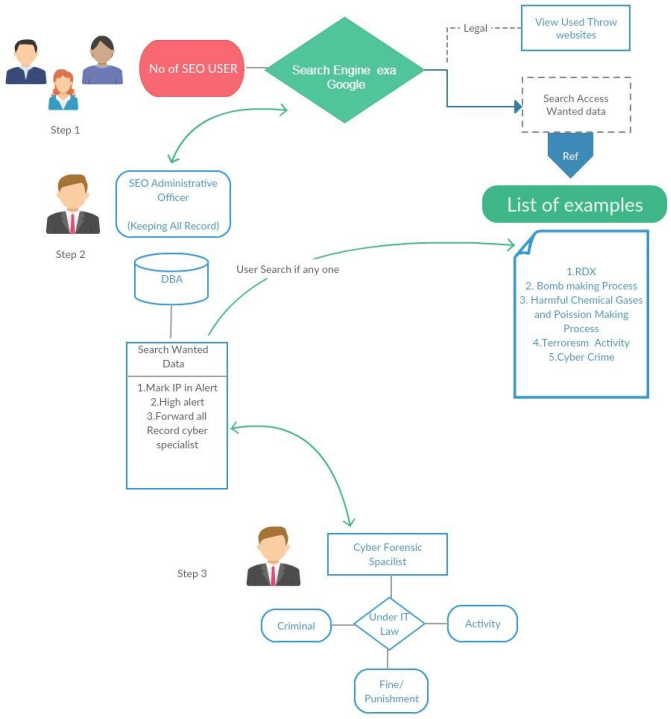

Fig.1 Flow chart of Search Engine Optimization Security Techniques under Indian IT Law

- **Role of SEO Administrative officer**
  SEO administrative officer monitors SEO database record and handle all activity, visit an user, Collaborate with development teams to discuss, analyse, or resolve usability issues coordinating bugs and legal activity.
- **Role of Cyber Forensic Expert**

  Cyber forensics expert is a branch of digital forensic science pertaining to evidence found in computers and digital storage media investigation and evidence. The goal of computer forensics is to aim on identifying, preserving, recovering, analysing and presenting facts and opinions about the digital information against a SEO criminal.

II. SEARCH ENGINE OPTIMIZATION ON PROPOSED WORK

From results point of view, according to process of Search engine, visitor searches data on SEO and searches required data on personal computer and also searches illegal data in Google SEO. As mentioned in Fig.2, all these information can be taken as an example, the number of times visitor visits SEO per Week and permits to access illegal information only three times, after that administrative officer restrict the IP & MAC Address of the user. Admin creates a database access directory in the form of user record in particularly illegal access [1], after that forward all above wanted records like access website (Name, Time, IP address, MAC Address) to Cyber Forensic Expert, who read a case study and Investigates and finally collect evidence and criminal is given fine –punishment under Indian IT act.

An Analysis of Search Engine Optimization (SEO) Security Techniques under Indian Cyber Law		
Google		
Search Information		(One weak Record)
10 Crores User- Visiter visit SEO Per/Weak in India		
Legal Information Access User	In legal Information Access user	Administrative Officer Keeping Record
(1) 99990000 per/weak	10000 per/weak 1st time	Data Base Alert Mark
(2) 99998500 per/weak	1500 per/weak 2nd time	Data Base High Alert Mark
(3) 99999700 per/weak	300 per/weak 3rd time	Data Base Read Mark & Carry Forward Cyber Forensic Specialist
Finally 300 user access In legal information Administrative Officer Forward List wanted user Cyber Forensic Specialist		

Fig. 2 SEO Categories on Search data - legal or Wanted

III. ROLE OF SEO ADMINISTRATIVE OFFCER

SEO Administrative Officer is an integrated suite of web promotion tools that cover all aspects of website optimization and promotion. An admin can handle all these activities related to SEO for marking process and secure monitoring and keeping records like Marking, Ranking, Paid listings, Page Rank, Pay-per-click (PPC), Indexed pages, illegal user IP & MAC address record and blocking under National Security showing concept in Fig.3.

3.1 SEO for User - A SEO user or visitor can work in SEO platform for searching a website, link address and find out a number of similar results according to a user, and SEO Administrative officer keeps all such record in the database. An Administrator officer maintains CIA Confidentiality, Integrity, and Availability for Security purpose and keep all visitors records in database, the user access a website or information on SEO for time and records. Admin maintain and rectified User access information which may be legal or illegal.

Fig. 3 SEO Administrative officer work

- **Legal Information Access: -** A SEO user access is used to throw on a website showing public and social and education purpose information used for a knowledgeable data access SEO, so that it does not affect a National Security, privacy or rule revolution for legal information on SEO.
- **Illegal Information Access:-** A SEO user accessing wanted information in the category of finding a RDX, Bomb making process, Harmful Chemical Gases, Terrorism Activity on the Internet, Cyber Crime data information access or affect National Security privacy or rule revolution access is illegal information on SEO, that is rectified by SEO Administrative officer
  - **Alert: -** if user accesses an illegal data first time in SEO; Admin keeps record in database and alert is marked from IP address and MAC address.
  - **High Alert: -** if user accesses the same category of illegal data second time in SEO, again admin keeps record in database in High alert for marking a IP address & MAC address.

- **Red Alert: -** if the user access the same category of illegal data for third time in SEO; Admin keeps a record in database Red alert is marked and IP & MAC address is restricted in SEO.

Red alert user data is forwarded to the cyber forensic specialist team and is applied a rule on revolution privacy access data information under Indian IT law.

IV. ROLE OF CYBER FORENSIC SPECIALIST

Cyber Forensics Specialist Investigator or Forensic Analyst are specially trained professionals who work with law enforcement agencies, or with private firms, to retrieve information from computers and other types of data storage devices.

Equipment may often be damaged either externally or corrupted by hacking or viruses internally. The Forensic Analyst is mostly known for working within the law enforcement industry; however, he or she can also be tasked to test the security of a private company's information systems. The Analyst should have an excellent working knowledge of all aspects of the computer but not limited to hard drives, networking, and encryption. Patience and the willingness to work for long hours are qualities that are well-suited for this position.

Fig. 4 shows the role of a Cyber forensic that can investigate a case and collect digital evidence and apply fine and punishment under Indian IT Law.

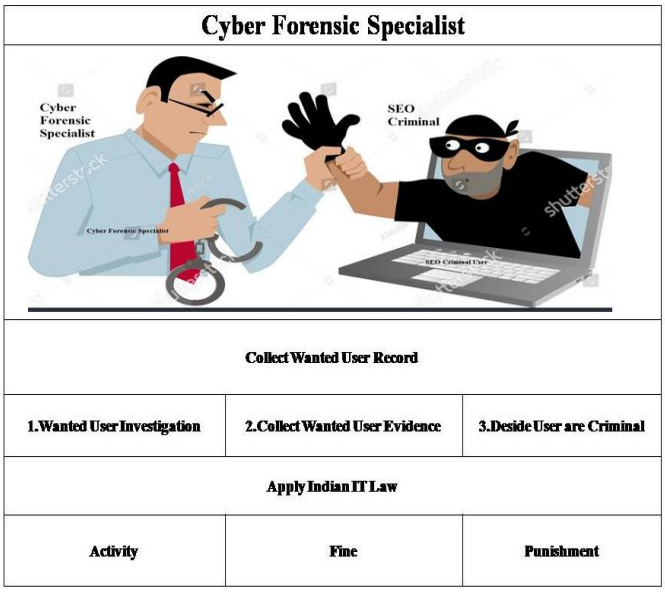

Fig. 4 Role of Cyber Forensic Specialist

4.1 Investigation

A cyber investigation is to provide sufficient evidence of the breadth and depth of the compromise to enable successful remediation of the affected [4] cyber crime areas and immobilization of the attackers.

Investigation is the process of law enforcement; officers use to track criminals via the computer. This process may be the process to investigate computer crimes or it may be to track records of criminals using computer forensic, mainly crime investigation is that to find out crime related evidence or to find answer.

All the 7W words are enumerated below.

1. What
2. Where
3. Who
4. When
5. Why
6. How
7. Answer

4.2 CYBER CRIME DIGITAL EVIDENCE

Cyber forensic specialists collect crime evidence spot point in computer web browser history record, hard disk, email header, IP Address and other investigation important role. “Evidence” means all computer records like file as image, Audio, Video, documentary electronic produced in court are called evidence. There are four types of evidence-

- **Real:** Real evidence is something you could actually carry into court and show to a jury. This type of evidence is the most powerful. Real evidence typically “speaks” for itself.
- **Documentary:** Documentary evidence is any evidence in written form.Database files, server logs, e-mail etc. Documentary evidence could be faked by a skilled computer user and therefore must be authenticated to be admissible in court. Always produce the original document, not a copy.
- **Testimonial Evidence:** Testimonial evidence is the statement of a witness, under oath, either in court or by deposition. This type of evidence typically supports or validates the other types.
- **Demonstrative Evidence:** Demonstrative evidence recreates or explains other evidence. Demonstrative evidence does not “speak for itself” and is used to illustrate and clarify previous points. This type of evidence is most helpful in explaining technical topics to non-technical audiences.

4.3 CYBER CRIMINAL

A cybercriminal is an individual who commits cybercrimes, where he/she makes use of the computer either as a tool or as a target or as both. Cyber criminal take action or computer play role of an illegal activity that access a data and damage it.

Cybercriminals use computers in three broad ways:

- Select computer as their target: These criminals attack other people's computers to perform malicious activities, such as spreading viruses, data theft, identity theft etc.
- Uses computer as their weapon: They use the computer to carry out "conventional crime", such as spam, fraud, illegal gambling, etc.
- Uses computer as their accessory: They use the computer to save stolen or illegal data.

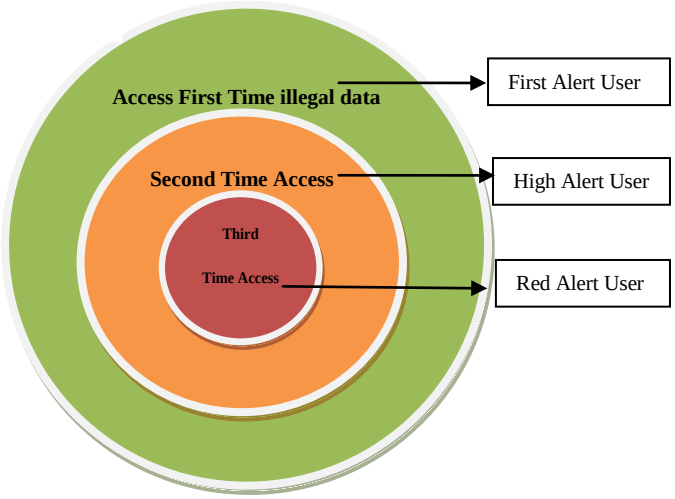

Fig.5. SEO Illegal User COUNTS Record

Cyber Forensic specialists investigate the case and decide according to evidence that SEO user is criminal or not. Cyber Forensic Specialist finds out all criminal records by applying IT Law at user's end. Fig.5 shows all records, first Alert user, second high alert user, and third red alert user as per the record of cyber forensic expert. In red alert user case, it investigate and collect all digital evidence to decide the user is criminal and apply Indian IT law under fine and punishment.

V. CYBER LAW IN INDIAN CONSTITUTION

In India, cyber laws are contained in the Information Technology Act, 2000 ("IT Act") which came into force on October 17, 2000. The main purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of Electronic records with the Government.

The following Act, Rules and Regulations are covered under cyber laws:

1. Information Technology Act, 2000
2. Information Technology (Certifying Authorities) Rules, 2000 [3]
3. Information Technology (Security Procedure) Rules, 2004
4. Information Technology (Certifying Authority) Regulations, 2001

5.1 OVERVIEW OF RULES ISSUED UNDER THE IT ACT, 2000

- **Information Technology (Certifying Authorities) Rules, 2000**
  This rule deals with licensing of Certifying [12] authorities and the procedures that need to be complied by them. It also prescribed the eligibility, appointment and working of Certifying Authorities.
- **The Information Technology (Certifying Authority) Regulations, 2001**
  The regulation details the technical standards and procedures to be used by a Certifying Authority.
- **The Information Technology (Other Standards) Rules, 2003**
  The rules deal with the standards to be observed by the Controller to ensure that the secrecy and security of the Digital signatures are assured.
- **The Information Technology (Security Procedure) Rules, 2004**
  These rules prescribe the provisions relating to secure digital signatures and secure electronic records.
- **The Information Technology (Use of electronic records and digital signatures) Rules, 2004**
  These rules deal with the manner and format in which the electronic records should be filed, created or issued. It also states the manner or method of payment of any fees or charges for filing or creating any electronic record.
- **The Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009**
  It contains the procedure for aggregate monitoring of communications and the procedural safeguards to be observed in them.
- **The Information Technology (Procedure and Safeguards for interception, monitoring and decryption of information) Rules, 2009**
  These rules explain the procedure and safeguards subject to which such interception or monitoring or decryption may be carried out.
- **The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public), 2009**
  The rules provide for the designation of an officer of the Central Government [3] for the purpose of issuing direction for blocking of access by the public any information generated, transmitted, received, stored or hosted in any computer resource. It provides the procedure and the safeguards to be followed by the designated officer.
- **The Cyber Appellate Tribunal (Procedure for investigation of Misbehavior or Incapacity of Chairperson and Members) Rules, 2009**
  These rules provide for the procedure for investigation of misbehaviour or incapacity of the Chairperson and members of the Cyber Appellate Tribunal.
- **The Cyber Appellate Tribunal (Salary, Allowances and other terms and conditions of service of Chairperson and Members) Rules, 2009**
  These rules provide for the salary, allowances and terms of service of the Chairperson and members of the Cyber Appellate Tribunal.
- **The Information Technology (Guidelines for Cyber Cafe) Rules, 2011**
  According to these guidelines, cyber cafes should register themselves with an appropriate government agency, and [40] provide services to users only after establishing their identity. It also deals with maintenance of records of such identity as well as log of sites visited, among others.
- **The Information Technology (Intermediaries guidelines) Rules, 2011**

These rules provide the rights and responsibilities of internet intermediaries in India. If the Internet intermediaries follow these rules and exercise proper cyber due diligence, they are entitled to a "safe harbour protection". Otherwise, they are liable for various acts or Omission occurring at their respective platforms once the matter has been brought to their notice.

- **The Information Technology (Electronic Service Delivery) Rules, 2011**
  These rules provide for creation of a [3] system of electronic delivery of services. Under the Electronic Service Delivery Rules the government can specify certain services, such as applications, certificates, licenses etc, to be delivered electronically**.**
- **The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011**
  These rules are regarding sensitive personal data or information and are applicable to the body corporate or any person located within India. It basically requires entities holding sensitive personal information of users to maintain certain specified security standards

VI. UNDER IT ACT FINE & PUNISHMENTS

Table-1 Indian IT Crime Against Cyber Law

Cyber Crime	Brief Description	Relevant Section in IT Act	Punishments
Cyber Stalking	Stealthily following a person, tracking his internet chats.	43, 65, 66	3 years, or with fine up to 2 lakh
Cyber Pornography including child pornography	Publishing Obscene in Electronic Form involving children	67, 67 [3]	10 years and with fine may extends to 10 lakh
Intellectual Property Crimes	Source Code Tampering, piracy, copyright infringement et	65	3 years, or with fine up to 2 lakh
Cyber Terrorism	Protection against cyber terrorism	69	Imprisonment for a term, may extend to 7 years
Cyber Hacking	Destruction, deletion, alteration, etc in a computer resources	66	3 years, or with fine up to 2 lakh
Phishing	Bank Financial Frauds in Electronic Banking	43, 65, 66	3 years, or with fine up to 2 lakh
Privacy	Unauthorized access to computer	43, 66, 67, 69, 72	2 years, or with fine upto 1 lakh

VII. CONCLUSIONS

The implementation of layout as the Internet continue to grow, the availability of information will also continue to increase dramatically. There needs to be order if people must find what they're looking for online. For this reason, search engines continue to occupy a critical "a prominent position" in the online world. They will continue to be part of the everyday lives of most people and will only become more important and necessary so people can find information more easily.

The SEO will work on local countries domain based on Indian security aspects under which if a user searches any illegal information in their SEO, then the Indian administrative officer and cyber forensic expert will be coordinate all security prospects as under IT law

REFERENCES

[1] Search Engine Optimization with Efficient Page Ranking Algorithm by Miss. Gayatri Vivekrao Kpase Dr. V.M.Thakre. National Conference on "Advanced Technologies in Computing and Networking"-ATCON-2015

[2] Cyber Crime Investigation Field Guide – By Bruce Middleton.

[3] http://www.cyberlawsindia.net/cyber-india.html

[4] Research paper of Cyber Crime and Security Soumya Tiwari, Anshika Bhalla, Ritu Rawat.

[5] http://deity.gov.in/ - Department of Electronics and Information Technology, Govt. of India

[6] http://catindia.gov.in/Default.aspx - Cyber Appellate Tribunal

BIOGRAPHIES

Anuraj Singh
MS Scholar, University Institute of Technology, BU, Bhopal, MP, India

Mr. Jay Narayan Thakre
Asst. Prof. Dept of I.T.
University Institute of Technology, BU, Bhopal, MP, India

Dr. Taruna Jain,
Head of Department, Cyber Law & Information Security,
University Institute of Technology, BU, Bhopal, M.P.