iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 1 **Issue:** II **Month of publication:** September 2013

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

Cyber Security in India'sTourism

Peeyush Vyas

Vadodara Institute of Engineering, Kotambi, Halol Road, Vadodara, Gujarat. India. peeyushvyas@gmail.com

Abstract: *The growing use of ICT for administration of all the spheres of our daily life cannot be ignored. Also, we also cannot ignore the need to secure the ICT infrastructures used for meeting social function like Tourism.*

Tourism is a very large industry in India. India has the fifth rank among countries with the fastest growing tourism industry according to the data given by World Travel and Tourism Council. Every year thousand of foreign tourists arrive in India mainly from Union Territories, Unites States and UK. Also, domestic tourists visit the states like Uttar Pradesh, Andhra Pradesh, Tamil Nadu, Himachal Pradesh, Jammu & Kashmir, Chennai, Delhi, Mumbai and many more places. So, the threat of Cyber Security in India's tourism has put an immense challenge during the last so many years. The threat attacks in resorts, hotels, banks, tourist offices and across all the major tourist places have become an inadequate mechanism to address this challenge.

The roll of ICT (Information and Communication Technology) has exposed the users to a huge data bank of information regarding their bank a/c number, credit/debit card number, contact number or any type of personal information etc. and all these information are very much vulnerable if we talk about the use of computers and internet in the field of tourism and hence the probability of cyber attacks cannot be denied.

This paper is in regard with the understanding of the nature and effectiveness of cyber security and making an effort to address this challenge, highlighting what could be done. With the advanced development in the country and with the use of tools like email, online shopping, cell phones, satellite phones, on line ticket booking, online reservations etc. , cyber security has become an important issue related to the cyber tourism. The electronic gazettes like computers, laptops, mobiles etc. are being used as a weapon. It is generally unlawful attack and the related threats against the computers, networks & information stored, and cause enough harm to generate fear amongst the local as well as foreign tourists.

Keywords: *Tourism, Cyber, ICT, Security*

1. INTRODUCTION

Cyber security can be described as the protection of systems, networks and data in cyber space. It is concerned with the protection against cyber risks, which broadly fall into three areas: Cyber Crime, Cyber War, and Cyber Terror. The growing use of ICT for administration of all the spheres of our daily life cannot be ignored. Further, we also cannot ignore the need to secure the ICT infrastructures used for meeting these social functions. Cyber security is in fact protecting our personal information or any kind of digital asset stored in computer or in any digital storage device. Here, it is a small try to elaborate cyber security in the area of India's tourism.

Tourism is a very large industry in India. India has the fifth rank among countries with the fastest growing tourism industry according to the data given by World Travel and Tourism Council. Every year thousand of foreign tourists arrive in India mainly from Union Territories, Unites States and UK. Also, domestic tourists visit the states like Uttar Pradesh, Andhra Pradesh, Tamil Nadu, Himachal Pradesh, Jammu & Kashmir, Chennai, Delhi, Mumbai and many more places. The threat of Cyber Security in India's tourism has put an immense challenge during the last so many years. The threat attacks in major tourist places, resorts, hotels and across all the major tourist places have become an inadequate mechanism to address this challenge.

The roll of ICT (Information and Communication Technology) has exposed the users to a huge data bank of information regarding their bank a/c number, credit/debit card number, contact number etc. and all these information are very much vulnerable if we talk about tourism and hence the probability of cyber attacks cannot be denied.
Reports suggest that cyber attacks are understandably directed toward tourism department as there is a great involvement of Indian as well as foreign currencies and hence it can collapse the Indian economy. This paper is in regard with the understanding of the nature and effectiveness of cyber security and making an effort to address this challenge, highlighting what could be done.

The structure of the paper will be as follows:

Cyber Tourism

In general, 'Cyber tourism' is the combination of tourism and cyber space. With the advanced development in the country and with the use of tools like email, online shopping, cell phones, satellite phones, on line ticket booking, online reservations etc. , cyber security has become an important issue related to the cyber tourism. The electronic gazettes like computers, laptops etc. are being used like a weapon. It is generally unlawful attack and threats against the computers, networks and information stored, and cause enough harm to generate fear amongst the local as well as foreign tourists.

Methods of Attack.

The Computer viruses, worms, hacking and fishing are frequently used as a weapon in the tourism industry . The attacks or methods on the computer system can be Syntactic or Semantic. In the Syntactic Attack the computer infrastructure is damaged by modifying the logic of the system in order to introduce delay or make the system unpredictable. Computer viruses and Trojans are used in this type of attack whereas in Semantic Attack the information keyed in the system during entering and exiting the system is modified without the users knowledge in order to induce errors.
Cyber tourism is not only limited to paralyzing computer infrastructures but it has gone far beyond that. It is also the use of computers, Internet and information gateways - to support the traditional forms of tourism like suicide bombings. Internet and email can be used for organizing a terrorist attack also. Most common usage of Internet is by designing and uploading websites on which false propaganda can be pasted. This comes under the category of using technology for psychological warfare.

Tools of Cyber Tourism.

Cyber criminals use certain tools and methods to allow to run freely this new age of tourism.
These are :-
(a) Hacking:-This is the most popular method used by a terrorist. It is a generic term used for any kind of unauthorized access to a computer or a network of computers. Password cracking, packet sniffing etc are the tools of hacking.
(b) Trojans:-These are the programmes which pretend to do one thing while actually the are meant for doing something different.
(c) Computer Viruses:- These are computer programmes, which infects other computer, programmes by modifying them. They spread very fast.
(d) Computer Worms:-They are a set of programmes that is able to spread functional copies of itself usually via network connections.
(e) E-Mail Related Crime:- Certain emails are used as host by viruses and worms. E-mails are also used for spreading disinformation, threats and defamatory stuff.
(f) Denial of Service:- These attacks are aimed at denying authorized persons access to a computer or computer network.
(g) Cryptology:- Cyber Criminals have started using encryption, high frequency encrypted voice/data links etc.

Challenges to National Security:

India has already made its position in the world related to the IT sector and has started in the working environment of e-governance and handling the tasks of 'Passport', 'Visa' and many more. The sector of tourism is hence highly reliable on the e-governance. Also, the concepts of e-commerce and e-banking have been brought in the new challenging areas. Indian tourism is highly based on these above mentioned factors. To paralyze the tourism segment all the possible mentioned threats are the delicate issues.

Existing Cyber Security Initiatives:

The various government organizations working for cyber security are as under -
National Informatics Centre (NIC):-

It is the organization that provides e-governance and network facilities to the Central Government, State Governments, Union Territories, Districts and other Governments bodies. Mainly, it provides ICT services in government bodies.

Indian Computer Emergency Response Team (Cert-In):-.

This is the major element of India's cyber community. Basically, it provides the main authorization for the cyber space through the secure communications and ensures the security for the cyber space.

National Information Security Assurance Programme (NISAP):-

NISAP is mainly for Government as well as typical infrastructure. Under this programme, it is mandatory for organizations to implement security control and inform to Cert-In if there is any security issue. Cert-In creates a panel which audits to the organizations.

Indo-US Cyber Security Forum (IUSCSF):-

Indo-US Cyber Security Forum was established in April 2002 as a step to intensify the on-going cooperation to address national security issues arising from the increasing interdependency of our critical network information systems involved in outsourced business processing, knowledge management, software development and enhanced inter-government interaction. The group is mandated to cooperate on policy, procedural, and technical issues of cyber security interest to both nations.

Challenges and Concerns :

Tracking of information available on the net has always been a tedious and a challenging task and looking to the present scenario of cyber traffic we can highlight the following concerns and challenges-

(a) Lack of general awareness of cyber security in tourism department at individual as well as departmental level.
(b) Lack of trained and qualified staff.
(c) A weak IT ACT with obsolete cyber laws.
(d) Non availability of email policies especially for defense, police and agency personnel.
(e) Cyber attacks from neighboring countries as well as criminals or rather educated criminals.
(f) Too many tourism organizations which have become vulnerable due to 'turf wars'.

Recommendations.

Certain recommendations are given below:-

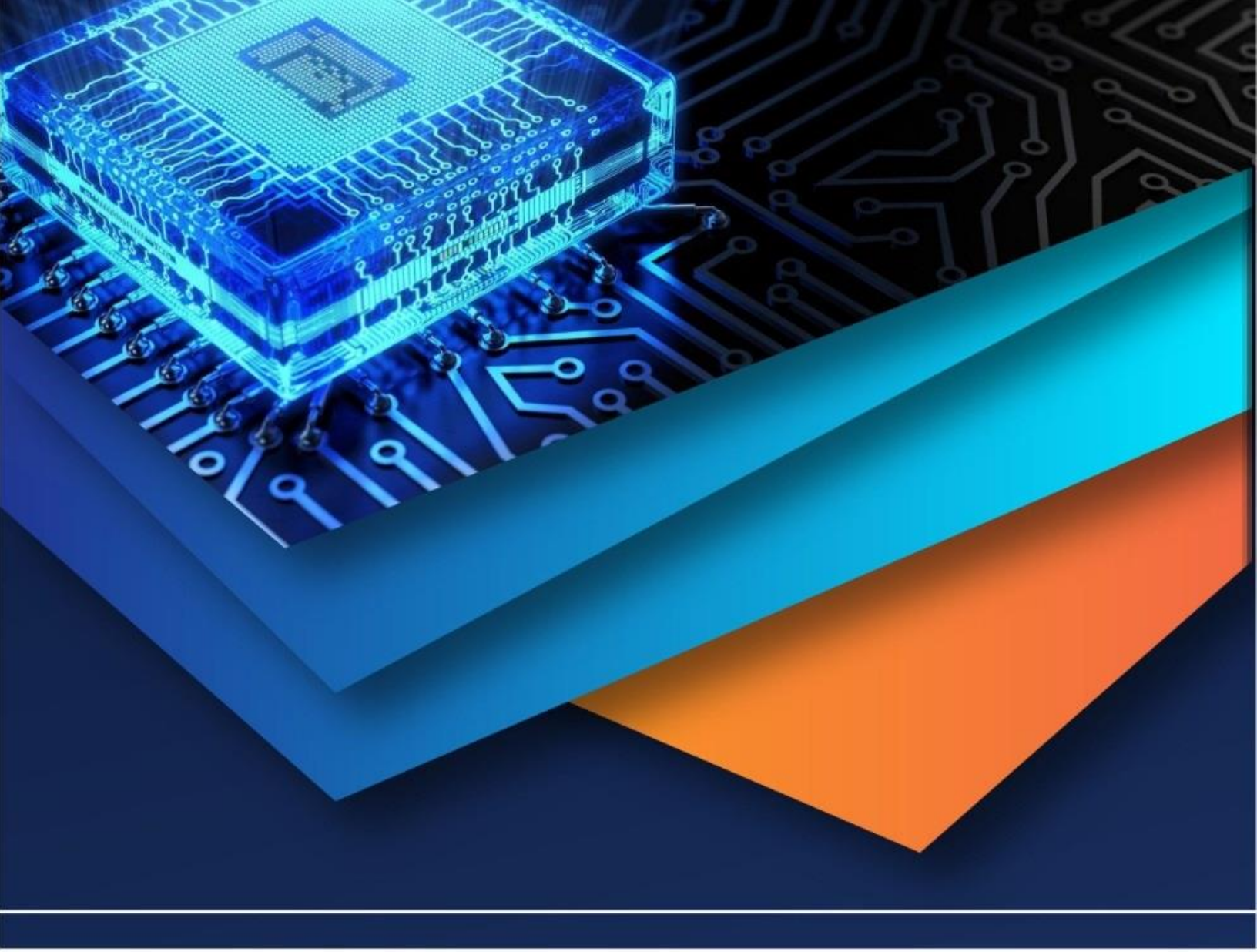
- ✓ Need to sensitize the common citizens about the dangers of cyber tourism.
- ✓ Cert-in should engage academic institutions and follow an aggressive strategy.
- ✓ Joint efforts by all Government agencies including defence forces to attract qualified skilled
- ✓ personnel for implementation of counter measures.
- ✓ Cyber security not to be given more lip service and the organizations dealing with the same should be given all support.
- ✓ Agreements relating to cyber security of India's tourism should be given the same importance as other traditional agreements.
- ✓ There should be more investment in the field of cyber security of tourism in terms of finance and manpower.
- ✓ Here should be a close eye on the developments in the IT sector by the Indian agencies working together in this direction.

Conclusions.

Google Nexus is a line of mobile devices using the Android operating system produced by Google in conjunction with several manufacturers. It is a series of smart phones and tablets manufactured by Google and its hardware partners and there is a growing nexus between the hacker and the tourists. The time will come when all the smart people associated with the tourism segment will be the good hackers. That will change the entire landscape of tourism. A common vision is required to ensure cyber security and prevent cyber crimes in the India's tourism. The time has come to prioritize cyber security in India's counter tourism strategy.

References

[1] Asian School Of Cyber Laws
[2] http://law.jrank.org/pages/11992/Cyber-CrimeIntellectual-property-theft.html
[3] http://zh.scribd.com/doc/45792947/Cyber-Crime-ppt
[4]http://www.virtualpune.com/citizencentre/html/cyber_crime_glossary.shtml
[5]http://zh.scribd.com/doc/60851869/13/Data-Diddling
[6]http://www.fotosearch.com
[7]http://articles.timesofindia.indiatimes.com/2012-07-16/ahmedabad



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY