Gurukul International Multidisciplinary Research Journal (GIMRJ)*with* International Impact Factor 8.357
Peer Reviewed Journal
DOI link - https://doi.org/10.69758/GIMRJ/2503I3IIVXIIIP0025

e-ISSN No. 2394-8426
Special Issue on Cyber Crime and Social Media
Issue–III(II), Volume–XIII

The pros and cons of ethical hacking from an Indian viewpoint

Dr.Murlidhar B.Rewatkar
Assistant Professor,Athawale College of Social work,chimur,Dist.Chandrapur-442903
*Corresponding Author Email: murlirewatkar1970@gmail.com
Contact: 9067979938

Abstract: The study's goal is to emphasize how crucial ethical hacking is. According to Jay Bavisi, CEO of the EC Council, "To counter the growing threat to IT security in the current globalized-digital era, all are in constant contact with ethical hackers." It is now understood by all parties involved that simply shutting your doors is not enough to secure a system. Using data from research journals, reports, news articles, and magazines that cover extensive collections of scholarly literature on the pros and cons of ethical hacking from an Indian perspective, the study used an exploratory research model based on previous literature. The report restates the urgent necessity to educate the nation's citizens on this worldwide issue in light of the emergence of international geopolitical disputes, financing of terrorist organizations, and cybercriminals' ability to compromise security systems and jeopardize national security.

Keywords: Ethical Hacking, cyber law, civil law, cyber terrorism, e-commerce.

INTRODUCTION: HISTORY AND EVOLUTION OF ETHICAL HACKING

The term "Ethical hacking" has first utilized in 1995 with the guide of IBM Vice President John Patrick, while the Ethical Hacker uncovered vulnerabilities in programming system to help endeavor proprietors fix the ones insurance openings sooner than a malignant programmer finds them. Many may contend that moral hacking is the point of the vast majority of the individuals of programmers, yet the present media discernment is that programmers are lawbreakers

1.1 The Origin of the Term Hacker

The records of moral hacking are accepted that programmers are digital and used to be a negative thought. The word surfaced in the ongoing past at the acclaimed Massachusetts Institute of Technology (MIT). Until Nineteen Sixties, hacking transformed into a timeframe utilized by understudy system to find exceptional strategies to top notch utilize the structures and machines to run them adequately. It's inventive side interest completed by means of some of the keen people inside the universal. The word criminal programmer originates before moral hacking.

1.2 Development of Phreakers and Tiger Groups

In Seventies the situation disintegrated with the creating notoriety of PC frameworks, individuals who got structures and programming dialects have been starting to see the conceivable outcomes in testing the ones frameworks to secure their capacities. So by then "phreaking" started to increase enormous un savoriness. Phreaking alludes back to the activity of controlling media communications structures. Begun to perceive cellphone systems, they raised to abuse the advantages and the organizations headed out to experience misfortunes where long separation calls become free with hacking cell phone systems. From the outset time that hacking changed into utilized for unlawful capacities by method for a huge amount of people. Henceforth, governments and enterprises all began to glance the advantage in having specialized specialists effectively are searching for out the shortcomings in a framework, letting them settle those issues

before they can be abused. They are as "tiger groups" and the American government turned out to be especially excited on the use of them to strengthen their ambushes.

1.3 The Rise of Black Hat Hacker

In 1990s, the word programmer started to be identified with hoodlum intrigue. The alleged acknowledgment of the PC as gadget for enterprises and people planned that various fundamental data and information were presently put away now not in substantial structure anyway in PC programs. Programmers began to peer the chances of taking insights that could then be purchased on or used to dupe organizations. Programmers have been unmistakable as hoodlums – virtual trespassers – who were the utilization of their abilities to advantage get right of passage to PC frameworks, steal data or even extortion companies into conveying monstrous aggregates of cash. These assortments of programmers are what we portray today as dark cap programmers: they might be absolutely intrigued by the utilization of their gifts for vindictive capacities and routinely connected to a wide range of criminal games. Dark cap programmers get the great estimated greater part of media intrigue, and there have been over the top profile hacks **1.4 Multifaceted Present Day Digital Hackers**

It is normal that more noteworthy than 30,000 sites are hacked each and every day, which goes to uncover the size of bleeding edge hacking and how it might affect associations all things considered. Programmers assortment from unpracticed "content kiddies" utilizing hacking hardware composed by method for others to best in class present day cybercriminals who will forestall at nothing to get what they need.

1.5 The Renaissance of the Moral Programmer

As programmers have come to be more brilliant and increasingly industrious, it has rise as increasingly more need of great importance for enterprises to have alright resistances contrary to them. In this way, the idea of moral hacking an expanding number of utilized by digital security organizations as an approach to battle the difficulty. Moral hacking is presently a not irregular speech it's miles feasible as of late to rise as Certified Ethical Hacker. The training is known as white cap hacking, and it includes utilizing the indistinguishable procedures that dark cap programmers use so as to hinder down digital guards. The differentiation is that when a white cap programmer has undermined the ones resistances they tell the matter of the manner in which they figured out how to do it all together that the defenselessness can be consistent.

1.6 How Good Ethical Hackers can help Organizations

It's anything but difficult to perceive how gatherings can pick up from the use of good programmers. A white cap programmer can copy a genuine digital ambush that dark cap programmers would attempt to play out the use of the entirety of the indistinguishable procedures that a real assault would utilize. In the event that a business' safeguards have a shortcoming, the moral programmer may be able to uncover it all together that it might be fixed sooner than a genuine hack occurs.

1.7 Moral Hacking Strategies

Moral programmers for the most part require a specific level of mystery to play out their occupations effectively, this implies they may regularly be contracted immediately by means of organizations' control without the comprehension in their workforce or digital security

gatherings. This mystery allows in a white cap programmer to work inside the equivalent way that a dark cap programmer could. They utilize an assortment of methods trying to beat the framework. Normally this could contain infiltration testing, in which they will utilize their expertise of coding and acclaimed vulnerabilities to attempt to profit get right of passage to. Much the same as dark cap programmers, moral programmers will attempt to utilize secret phrase breaking just as social designing. Hacking might be utilized as an unlawful weapon to figure out the codes of any site, switch online cash illicitly, getting out secret messages and distinctive limited stuffs as appropriately. To stop such things Ethical Hacking is been coordinated inside the PC structures. In layman Ethical Hacking intends to hack inside the Limits, i.E. Hacking up to which there's no misfortune to every other person. The study divided in to four parts, first part is about the history and evolution of the Concept Ethical hacking and its relevance in the current era of internet. Second part is about the literature review of the study and gives a glimpse of types of hackers. Third part is about Ethical hacking in India and the fourth part offers conclusion. on enormous associations like eBay and Sony in current years.

1.8. Objective of the Study

Ø To study the good and bad aspects in ethical hacking and its importance in India

Ø To offer Policy Suggestions

1.9 Limitations

The study is confined to describe the pros and cons of the term ethical hacking and it's applicability in the Indian perspective. The literature review collected is the base for drawing conclusion.

2. LITERATURE REVIEW

DANISH JAMIL AND MUHAMMAD NUMAN ALI KHAN (2011) tested is ethical hacking moral? And concludes that, the mind is a very powerful tool that has no manage, the control will continue to grow proportionally with the preference to get knowledge of something this is impossible to achieve in its entity, however no longer forgotten in its entirety. Hackers will usually locate ways of getting into structures, whether or not they're doing it for precise or bad. NARENDER KUMAR CHAUHAN AND SUDHIR NARAYAN SINGH(2013) analysed Information Ethics within the Age of Information and Communication Technology. The look at concludes that technological improvements, no doubt demerits will come routinely. People can experience the lifestyles of deserves and they even attempt difficult for the establishment of equilibrium of balancing between deserves and demerits and harms and advantages. The mature experience of cosmopolitan citizenship and a deep rooted moral sense of belongingness and sensible usages of ICT train network how to deal with with the information and statistics ethically and responsibly. In ICT era data floating is veryfast and the identical is ideal as well but at the opposite from time to time the facts flows are used unethically although customers convey true intentions. DAMA ANAND AND AKKI SURESH BABU (2014) studied network safety and commercial enterprise protection through moral hacking and conclude that the unexpectedly advancing sophistication stage of cyber threats corporations cannot come up with the money for to depend upon untested and unproven protection architectures. Businesses must increase the effectiveness in their protection architectures to the factor that they may now not be focused for

hackers. The aim should be to achieve a security architecture that could require sufficient of the attacker's assets to penetrate that would price the hacker more than the information is worth. CH. SUHASINI (2014) studied Ethical Hacking and its Vulnerabilities. Ethical hackers ought to discover vulnerabilities beforehand to minimize the threat. The organization should undertake penetration checks to locate if they're liable to assault. Finding vulnerabilities for organizations no longer simplest enables the organization but also minimizes the risks of assaults. She concludes that, era has persisted to develop at a excessive price through the years and maintains to achieve this; scholars are putting themselves in inclined positions by supporting people to hack. The thoughts is a totally effective device that has no control, the manage will keep growing proportionally with the choice to get information of something this is not possible to reap in its entity, however not forgotten in its entirety. V.CHANDRIKA (2014) analysed types of ethical hackers : A 'white-hat' hacker, also referred to as an ethical hacker, is someone who has non-malicious intent whenever breaking into security systems. The majority of whitehat hackers are security experts, and will often work with a company to legally detect and improve security weaknesses. A 'black-hat' hacker, also known as a 'cracker', is someone who hacks with malicious intent and without authorisation. Typically the hacker wants to prove hacking abilities and will commit a range of cybercrimes, such as identity theft, credit card fraud and piracy. A black hat hacker is an individual with extensive computer knowledge whose purpose is to breach or bypass internet security. A 'grey-hat' hacker is somewhere between white-hat and black-hat hackers, as he or she exhibits traits from both. For instance, a grey-hat hacker will roam the Internet in search of vulnerable systems; like the white-hat hacker, the targeted company will be informed of any weaknesses and will repair it, but like the black-hat hacker the grey-hat hacker is hacking without permission. A blue hat hacker is someone outside computer security consulting firms who bug tests a system prior to its launch, looking for exploits so they can be closed. Elite hackers used an invented language called 'Leetspeak' to conceal their sites from search engines. The language meant some letters in a word were replaced by a numerical likeness or other letters that sounded similar. The 'best in the business' and are considered as the innovators and experts. Hacktivist is Someone who hacks into a computer network, for a politically or socially motivated purpose. The controversial word can be constructed as cyber terrorism as this type of hacking can lead to non-violent to violent activities. She concludes that the security problem will remain as long as manufacturers remain committed to current system architectures, produced without a requirement for security. As long as there is support for ad hoc and security packages for these inadequate designs and as long as the illusory results of penetration teams are accepted as demonstrations of a computer system security, proper security will not be a reality. Regular auditing, vigilant intrusion detection, good system administration practice, and computer security awareness are all essential parts of an organization‟s security efforts. A single failure in any of these areas could very well expose an organization to cyber-vandalism, embarrassment, loss of revenue or mind share, or worse. Any new technology has its benefits and its risks. While ethical hackers can help clients better understand their security needs, it is up to the clients to keep their guards in place. PANKAJ SHEORAN AND SUKHWINDER SINGH(2014) analysed Applications of Ethical Hacking and conclude that The Hacking has been a commonplace

phenomena in the community environment. The hacking can also be legal and ethical. They have mentioned the troubles of the hacking and how it may be made beneficial for dealing with the information resources over the Internet. The use of these strategies can protect the passwords , login names and different crucial statistics over the community it is taken or stolen with the aid of some different unauthorized character. The moral hackers have nice behaviour in the direction of the technology which may be utilized for locating the safety attacks and make use of their know-how for finding the misuse of technology in the laptop discipline. On the science of behavioral experience the humans are responsible for technological misuse and hacking being time period misused now we will observe the techniques of hacking for safety purpose. RANJINI MUKHOPADHYAY AND ASOKE NATH(2014) have studied the phenomenon Ethical Hacking: Scope and challenges in 21st century and concludes that Hacking preys on weak safety practices and undisclosed vulnerabilities. Firewalls, encryption, and digital personal networks (VPNs) can create a fake feeling of safety. These security systems often attention on high-stage vulnerabilities, which includes viruses and site visitors thru a firewall, without affecting how hackers paintings. Attacking one's own systems to discover vulnerabilities is a step to making them more cozy. This is the simplest established approach of substantially hardening one's systems from assault. If people don't identify weaknesses, it is a count number of time earlier than the vulnerabilities are exploited.

BISMA BASHIR AND AQEEL KHALIQUE (2016) had executed a assessment observe on safety versus ethics and concluded that Ethics ought to be accompanied and complied to fulfil protection goals in any agency. Security measures are quantifiable however the parameter of ethics is relative to the situations and entities involved. As a part of future paintings we would really like to focus on discrete ethical parameters governing quantifiable security targets. The discrete ethical variables may be derived through the use of fuzzy common sense, unsupervised getting to know and many others. MIGUEL ARMANDO HERNANDEZ BEJARANO AND ET.AL (2018) analysed moral hacking on cell gadgets and conclude that Ethical hacking is a device for statistics safety and prevention. Due to the proliferation of mobile gadgets, drugs and smartphones and the huge range of packages, the phenomenon of laptop lack of confidence has expanded extensively and therefore those are exceptionally susceptible. A new device isn't always that it is so remotely susceptible, if the person makes an ok handling of the telephone with out connecting to insecure networks, a good deal much less entering passwords on web sites that don't deal with encryption protection that make the tool an assault goal for the attacker can steal statistics, however the beginning of the attacks is because of the horrific manipulation of the consumer, nor does it serve to have port blockading by way of default or the deletion of permissions to put in unknown applications if the consumer offers permissions without reading or having know-how of what's which is installing making the telephone's security inclined.

3. ETHICAL HACKING IN INDIA

Before going into the legality of ethical hacking, we must keep in mind that hacking and ethical hacking is unique. Hacking is a wrongful act underneath Indian legal machine. Although ethical hacking is not so widespread in India but it's far an evolving profession. There are various institutes and schools in one-of-a-kind cities of India which offer publications of ethical hacking.

India emerged as the third maximum susceptible usa in terms of threat of cyber threats, such as malware, unsolicited mail, and ransom ware, in 2017, transferring up one location over the preceding year, consistent with a document by safety solutions issuer Symantec. Although Indian laws do not especially address ethical hacking yet hacking is a punishable offense in India. The act of Hacking contravenes the underlying ideas of India legal device. The issue of moral hacking has now not been treated explicitly in Indian laws, consequently, it loved neutral status underneath Indian criminal device.

3.1 Constitutional Disagreement

As in step with constitutional ideas hacking interferes with Article 21 which offers with the proper to existence and private liberty which includes right to live with dignity. Moreover, the act of hacking also infringes the right to privateness of an individual which is a fundamental proper now. Not a Crime

Two elements are required for the charter of a criminal offense and these two elements are

Ø mens rea i.E. Bad aim

Ø actus reus i.E. Bodily act.

In moral hacking, the first and the primary element i.E. Mens rea itself is missing, consequently, the question of it being a criminal offense does not arise. Moreover, moral hacking is achieved with the intention to save you hacking, therefore, it is important.

Trespass is mainly divided into 2 sections specifically

Ø Trespass to the person, and

Ø Trespass to assets.

For this newsletter, the only trespass to assets is applicable. The general definition of trespass states that it's miles an unauthorized intrusion upon the belongings of every other without the permission of the real owner. The trespass is a wrong below both the branches of legal guidelines i.E. Civil law and criminal regulation. In Civil legal guidelines, the purpose is irrelevant whereas in the latter goal is essential. The incorrect of trespass is the only offense that's regularly attributed to moral hacking however it's far truly relevant to the act of hacking and now not ethical hacking.

3.2 Civil Law

Under civil law, trespass approach entering within the property of every other without the permission of the owner. It is a part of the Law of Torts that's an unmodified law and primarily based at the case legal guidelines. Although the law of torts simplest covers tangible assets so it'll neither be relevant to hacking nor is it relevant to ethical hacking. In furtherance of the same, moral hacking does now not invoke any legal responsibility because it's far carried out with the permission of the proprietor so the query of it being a civil wrong will in no way get up. **3.3 Criminal Law**

Under Indian criminal law, trespass is described under phase 441 of Indian Penal Code (IPC), 1860 with a totally huge scope. In quick, it defines trespass as entering upon the assets of another with malice or so one can purpose some harm or to intimidate the owner of the involved belongings. Here, it is not exact that what sort of assets is wanted to constitute the crime of trespass.

Trespass is a wrong towards the belongings which is of sorts

Ø Tangible

Ø Intangible

Hacking is trespass to a pc gadget that's an intangible asset. Physical intrusion and bodily damage are not always essential to determine the legal responsibility for trespass. Nowadays pc device, software, websites all are construed as property. The expressions like homepage, touring a website, area or visiting to a site and many others. Are used inside the internet international; this shows that the web sites are property. Therefore any form of unauthorized intrusion on them with terrible intention can come under the purview of crook trespass. All the essentials consisting of motive to dedicate an offense or to intimidate, insult or annoy are absent in the act of ethical hacking, therefore, it's far criminal and doesn't invoke any legal responsibility.

3.4 Information Technology Act, 2000

Information generation (IT) Act, 2000 is a watershed motion in Indian legal system and a landmark within the cyber law arena. If we have a look at the provisions of IT act cautiously, we will deduce that it covers nearly all the wrongs that emerge from hacking because hacking is such offence which may be very extensive and covers numerous other offenses e.G. Someone who hacks the machine of some other man or woman can leak the private statistics of the owner, it can also be used to extort cash, a black hat hacker also can use the information to complement himself and so on. Chapter XI Section sixty six of IT Act, 2000 particularly deals with the act of hacking. Section 66(1) defines a hack as, any man or woman, dishonestly or fraudulently, does any act stated in Section forty three is referred to as hacking, and Section sixty six(2) prescribes the punishment for it. Hacking is a punishable offense in India with imprisonment up to three years, or with exceptional up to 2 lakh rupees, or with both. Chapter IX Section forty three of IT act, 2000 prescribes a penalty for the harm to pc or pc device. It is a common element which takes place each time a pc device is hacked. Black hats harm the device that they hack and scouse borrow the records. This enumerative provision consists of a whole lot of activities. Chapter XI Section 65 of the stated act makes tampering with laptop source files an offense. Section seventy two of the equal chapter makes the breach of confidentiality and privacy, a punishable offense. This is the most common aftermath of hacking.

The above-mentioned provisions obligatory the need of mala fide i.E goal to purpose damage that is absent in ethical hacking therefore moral hacking isn't always unlawful in India. India is ranked third among countries which can be going through maximum range of cyber threats as per safety software program firm Symantec. The same studies additionally ranked second in terms of centered assaults Keeping this records in thoughts, it's far unjustified to disregard the necessity and importance of ethical hacking inside the contemporary in the legal state of affairs. It is an offence way of hacking a networking gadget and has to paintings underneath some policies. As a ways because the governing guidelines are complied with, the act is justified. Furthermore, moral hacking includes the permission of the proprietor of the device and that is executed in compliance with the regulation which once more strengthens the criminal of moral hacking. The era we stay in is the technology of internet and internet of things: a laptop system is a domestic to limitless records and accounts so the chance is omnipresent. As a end result of this mass garage

of facts, our computer gadget desires to be up to date timely and required motion should be taken to save you black hats from gaining such information. Therefore ethical hacking is prison.

3.5 Ethical Hacking as a Profession

Cyber Security and Networking are booming Industries of the world today. Companies use the Internet to run them and control their activities. Internet usage has eased the work of such entities but at the same time, it also poses a chance to them. Thus the moral hacking is altogether a new career in itself and its developing each day. The dream of the digitized country similarly strengthens the want for moral hacking in India because it seeks utmost usage of the Internet. We want to remember the fact that cyber-security is a method and no longer a product and there's no server or cyber device that is past hacking. Everything on the net can b hacked relies upon upon the expertise of hacker and the efforts given. White hats work with the authorities and private firms to test their networks for vulnerabilities, loopholes, and insects to forestall an real black hat from encroaching upon the network. **3.6 Ethical Hackers are Employed Through Businesses to Hack their very Own Respective Enterprise**

In the age of information, the maximum dangerous things are the data itself. It is for your desire as long as you own it however as soon because it escapes and reaches to incorrect hands it overshadows another maximum dangerous matters. In such scenario, huge organizations face the biggest cyber safety threats from their competition. They always live underneath the hazard of their device being hacked. All the information referring to their commercial enterprise are saved on the server which if hacked can ramshackle the enterprise Ethical hackers are euphemistically called cyber security experts. The profession of Ethical hacking isn't always most effective restricted to IT agencies however different organizations also lease ethical hacker now. Companies like Wipro, Infosys and IBM Wipro, Infosys, IBM, TCS, Tech Mahindra, HCL, Airtel, Reliance are some of the examples of the groups which are regarded for moral hacker recruiters.

3.7 When Ethical Hackers are hired by Government as Cyber Security Experts

Nowadays authorities of different countries are going through a trouble with recognize to their cyber safety. Although Government of India does no longer provide Job of the moral hacker in any of its departments. In various authorities departments, cyber safety professionals are employed for the cyber-associated paintings. Moreover, numerous government organizations and wings of the military and regulation enforcement, protection groups, forensic laboratories, detective agencies, and investigative services need moral hackers. Investigative companies just like the Central Bureau of Investigation (CBI), the National Security Agency (NSA) and the Federal Bureau of Information (FBI) hire cyber security professionals however don't disseminate their statistics in public. Some of the government departments wherein authorities recruits cyber protection professionals are Department of Electronics and Information Technology and underneath which there may be ICERT (Indian Computer Emergency Response Team), Intelligence Bureau, Ministry of Communications & Information Technology, Department of Telecom, National Technical Research Organization, Defense Research and Development Organization, Army etc. This isn't always an exhaustive listing and nowadays different departments of government additionally want pc experts. There are right written checks and

interviews for such jobs. Cybercrimes in India nearly doubled in 2017, in keeping with facts launched by means of the National Crime Records Bureau (NCRB). The data comes inside the backdrop of India intending to come to be one thousand billion greenback virtual economy. Interestingly, cybercrimes accounted for much less than a percentage (0.43%) or 21,796 cases of a total of 50,07,044 cognizable crimes in 2017. Beneath Cyber Crimes towards Women & Children, NCRB is accumulating crime statistics below crime heads which includes Cyber Blackmailing / Threatening, Cyber Pornography, Cyber Stalking, Defamation / Morphing, Fake Profile, Internet Crimes thru Online Games, etc," the NCRB document said. With the Centre putting in the NIC-CERT--National Informatics Centre-Computer Emergency Response Team--to combat cybercrimes and the house ministry presenting to installation the Indian Cyber Crime Coordination Centre (I4C), the government is hoping to pork up India's cyber protection community (live mint -oct, 30 2019).

CONCLUSION

There is no legal definition of ethical hacking in India. Only after gaining a conceptual understanding of the laws governing hacking can one determine whether it is legal. It is possible to infer that ethical hacking is legal in India after testing it under the guidelines of both the criminal and civil laws. Crimes such as child pornography, phishing, credit card fraud, bank robbery, illicit downloading, industrial espionage, kidnapping children through chat rooms, scams, cyberterrorism, virus development and/or distribution, spam, and so forth. As a result, there are ongoing legal proceedings involving cybercrimes, reports of online money fraud, and the withdrawal of crores of rupees from banking servers. The government must act quickly to protect these resources by morally sound measures.

REFERENCES

[1] al, M. H. (2018). Ethical Hacking on Mobile Devices: Considerations and practical uses. International Journal of Applied Engineering Research, 16637-16647.
[2] Babu, D. A. (2014). Network Security and Business Protection through Ethical Hacking. International Journal of Emerging Technology in Computer Science & Electronics, 55-57.
[3] blog. (2019, august 12). ethics. Retrieved from blog.ipleaders.in: https;//blog.ipleaders.in
[4] Khalique, B. B. (2016). A Review on Security versus Ethics. International Journal of Computer Applications, 13-17.
[5] KHAN, D. J. (2011). IS ETHICAL HACKING ETHICAL. International Journal of Engineering Science and Technology, 3758-3763.
[6] livemint. (2019, october 30). cyber crime. Retrieved from livemint: www.livemint.com
[7] Nath, R. M. (2014). Ethical Hacking: Scope and challenges in 21st century. International Journal of Innovative Research in Advanced Engineering, 30-37.
[8] Singh, N. K. (2013). Information Ethics in the Age of Information and. International Journal of Information Dissemination and Technology, 249-253.
[9] Singh, P. S. (2014). Applications of Ethical Hacking. International Journal of Enhanced Research in Science Technology & Engineering, 112-114.
[10] staysafeonline. (2019, sep may). ethical hacking. Retrieved from www.staysafeonline: https:staysafeonline.org
[11] V.Chandrika. (2014). ETHICAL HACKING: TYPES OF ETHICAL HACKERS. International Journal of Emerging Technology in Computer Science & Electronics, 43-48.