A Study on Software Encryption of Aadhar Data with Special Reference to Right to Privacy and Constitutional Rights.

Author
Sanket Mohapatra
2nd Year, BA.LLB(HONS).
Saveetha School of Law
Saveetha Institute of Medical and Technical Sciences
Saveetha University
Contact: +91 9940552720
Email: sanket5879@gmail.com

Co Author
Shantilal Jain
2nd Year, BA.LLB(HONS).
Saveetha School of Law
Saveetha Institute of Medical and Technical Sciences
Saveetha University
Contact: +91 9360268498
Email: sslal2000@gmail.com

Abstract

There is a sort of legal confusion in society about Aadhar which can be understood from the title of the legislation. The confusion is limited to certain limitations because legal and cyber awareness about Sensitivity of Aadhar is not described in adequate. Though Digital India has brought a lot of advantages and developmental aspects to the society in lieu of a common man, it also brings with it great concern about privacy issues. The main concept of Aadhar is that everything is said to be done with biometrics and thus it gives a lot of security. But, the question is "Is Aadhar Secure"[1]. Because in this modern world, nothing is 100 percent secure in the field of information security and this Aadhar database if breached is a potential platform for grave danger. Also, biometrics can be fraudulently reproduced easily using simple resins to complex 3D printing techniques. Thus, the idea of Aadhar even though it is developmental, also has a dark side of security concerns that are still not properly answered.[2] Moreover with the concerns of safety there comes the concern for solution. In this research paper, we'll be focusing on how Aadhar and Cyber Policies are vulnerable to Cyber Threats without a Stringent Law to Protect Data Privacy and Individual Anonymity.

Keywords:- Data Protection, Cyber Knowledge, Privacy, Cyber Intrusion, Public Policy

INTRODUCTION

The Aadhar number i.e. The 12 digit unique identification number based on the slogan **"aam aadmi ka athikar"** was a lateral move by the central government and it was a major amendment bill which brought into existence yet another form of identification for the existing citizens of the country.[3] The Aadhar amendment bill was passed by the parliament in the form of Aadhar Amendment Act, 2016 to replace the existing ordinance issued in March 2019. Also said to be

[1] **REETIKA KHERA, *The Different Ways in Which Aadhaar Infringes on Privacy* (2017), https://thewire.in/government/privacy-aadhaar-supreme-court.**

[2] **Sandeep Shukla, *Aadhaar verdict: Why privacy still remains a central challenge* (2018), https://economictimes.indiatimes.com/news/politics-and-nation/aadhaar-verdict-why-privacy-still-remains-a-central-challenge/articleshow/65970934.cms?from=mdr.**

[3] **(*Aadhaar-privacy debate: How the 12-digit number went from personal identifier to all pervasive transaction tool*, 2018)**

for the convenience of the public, this Aadhar will also be allowed as a ue of KYC for bank customers in various governments and amendments relating to this was made under the Telegraph Act, 1885 and the Prevention of Money Laundering Act, 2002. Also as an address to the concerns relating to minors it was said that a minor can oop out of this biometric identification system, That is the Aadhar system on attaining the age of 18 years. Even though this aadhar was supposed to be people friendly, it also led to a nationwide agitation when the privacy issues of it were talked upon. Moreover, it is said that this database is supposedly 100% safe and will not get into the wrong hands. But the major concern is that the collection of this Aadhar database is in itself done through private entities and agencies and it calls for a speculation that whether the government is acting to its fullest in addressing the privacy issues in this context. Moreover, when it comes to terrorism and illegal immigrants,[4] Those people are a certain risk to the social security of a country. But in some instances terrorists and illegal immigrants were themselves found to be in possession of this Unique Identification Number in their names. This caused a lot of speculation about whether the government is acting to its fullest in securing the aadhar reaching the wrong hands. If done so, how did these illegal immigrants come into possession of this Unique identification number with their biometrics in it? Also, this in itself is enough to get them various social benefits and has the potential to mask them as citizens of this country. This is a great concern of security and requires addressing to become. This is a serious security issue[5] where in one instance terrorist from Jaish-e-mohammed terror group was in possession of an aadhar card[6] in an alias with him at the time of arrest. There are many instances like this which are a grave concern for the privacy and security issue of Aadhar. This in itself proves that the security is not enough in case of aadhar. Also nowadays aadhar is the key to all governmental and non governmental services. Aadhar alone can give the status of an individual to a person. In that case, the measures here seem to have failed no matter what the layer of security has been given to the database. Maybe, the main cause of these issues

[4] **Privacy Concerns Over Your Aadhaar Card, (2018), https://www.youthkiawaaz.com/2018/08/privacy-concerns-over-your-aadhaar-card-explained/.**

[5] **Suhrith Parthasarathy, *A renewed attack on privacy: on Aadhaar Bill* (2019), https://www.thehindu.com/opinion/lead/a-renewed-attack-on-privacy/article25943864.ece.**

[6] **Jaish-e-Mohammed terrorist from PoK caught, Aadhaar card recovered from him, (2018), https://economictimes.indiatimes.com/news/defence/jaish-e-mohammed-terrorist-from-pok-caught-aadhaar-card-recovered-from-him/articleshow/52279688.cms?from=mdr&utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst.**

may be the grant of private agencies the right to collect the aadhar database. Yes. Even till date the government has tied up with private agencies in helping them with the collection of aadhar database. How can the government, in such a sensitive issue, grant private access to other private entities which can cause misuse of sensitive data.The Software Encryption of an Application which can save the data to a certain limit and third parties cannot know about the conversation is a good data restriction but the question is “If the App Developer Entity doesn’t know about the conversation where is the information stored if not in the server of the software”. We have a digital India where we are a part of the computer and computer is a basic necessity of our life. But, whether Digital India is a Secure Digital India is a matter of speculation and question of cyber security. Aadhar linking to a software or social media platform can prove to be a cyber threat. Encryption can be broken with decryption code which a systematic analysis of data source can reveal in seconds. Our Country doesn’t have a Data Protection Law yet and the sovereign authority reason that our database freedom is being monitored and supervised on behalf of surveillance to protect the integrity and sovereignty of our country in the cyber front from external threats which can affect our Information System by extracting crucial national interest details. Moreover, folks at Information Technology University’s and the rest of the Cyber field claim that even though the data in social media is end to end encrypted like in the case of What’sApp, the origin of the source message can be tracked out by decryption. If that is the case, where is the privacy in this case. Also, with this, the government’s initiative to interlink Aadhar with social media accounts may seem to give the remedy to finding offenders. But, it is also a great kick start for Cyber Criminals to focus their attacks on individual people. The main idea of social media is to have a freedom of speech and expression combined with internet rights. If that main idea behind the existence of social media goes haywire, then what is the benefit out of it. We all are familiar that already people are vulnerable over cyberspace no matter what the amount of security is out there. The very profound example of this instance is the **wannacry** ransomware which caused a lot of financial loss to many countries who were proud of their cyber security measures, but all went in vain. Also, we hear a lot of news now and then where people use social media to commit various forms of crimes starting from sex Offences to even there are speculations of trafficking using social media. In that case, if the Aadhar database as proposed by the government is linked with social media, then where is the privacy there? Also, this will be like giving our own address for a burglar to come and lift off our identity which is at stake here. AADHAR AND SOCIAL MEDIA : Moreover, when all about social media comes into play, almost all the social-media that is in constant public use are private entities. Also, in this modern era of Cyber tech growing at an exponential rate and wide range of Artificial Intelligence capabilities, social media also possess a significant threat to the identity of people. Already these social media contain loaded information about the user than a person very close would know about that person. And the further addition of Aadhar Identity towards social media, is not a small matter. Offenders would have access to almost the whole bio of a person combined with their Aadhaar numbers and what not. Nowadays there are various spybots that are being deployed over the internet in disguise of some other application. These spybots use AI and go beyond the recognition of the user and collect real-time information like even the psychology of that person. Combined with all this information, it would be a smoking gun in the hands of criminals. Thus, the addition of Aadhar in social media is a great risk.

Objectives

Software Encryption has some substantial questions of law :

- **To identify the disclosure is known to a Trustworthy Person**
- **To observe whether your sensitive cyber information is in reliable hands**
- **To discover the legality that your personal details will not be misused against yourself which will be in Contravention of Article 20(3) of the Constitution of India.**

Review of Research Literature

The Research Paper Focuses on the legality and constitutionality of disclosure of sensitive information to state controlled machinery and the propositions laid in the Aadhaar Case is abided by the government or not. Data Privacy has been a legal evolution in recent times with development of advanced Information Technology Systems in the country and internet data misuse by third party groups. Information Technology has many legal restricts and the discrepancies in the IT Act,2000 has been widened by the 2008 Amendment which was widely debated because of its controversial nature and clampdown on data privacy.

The Research Paper Identifies the problematic nature of the aadhaar act and its need and interpretation of the name of the statute as a subsidy provision statute. It determines the identity of an individual but is not a proof of citizenship and it also discusses the problem of software encryption because it can be used for cybercrime purposes. Aadhar Data is the most sensitive data and the poor storage of aadhaar data can cause chaos across the country because the significance of the data is known by the Aadhaar Holder and not by the person misusing it. There is no explicit legal provision to protect any victim of any criminal activity in which he has been falsely implicated due to the presence of his Aadhaar Data in the specific crime scene.

The Research Paper discovers the vague nature of the software encryption by Third-Party Groups and their liability in mishandling the data has not been deliberated by any lawmaker. It should have any socio-legal consistency. It should not be used for illegitimate purposes and more significance to Aadhaar during the presence of other valid ID Proofs like Pan Card, Voter ID, Land Documents, Passport, Birth Certificate, Driving License and MGNREGA Card are also alternate ID Proofs. The Software Encryption of Aadhaar Data increases the Legal Burden on any individual due to inefficiency of the appropriate authorities in providing an Quasi-Judicial Assurance to the People has not been fulfilled.

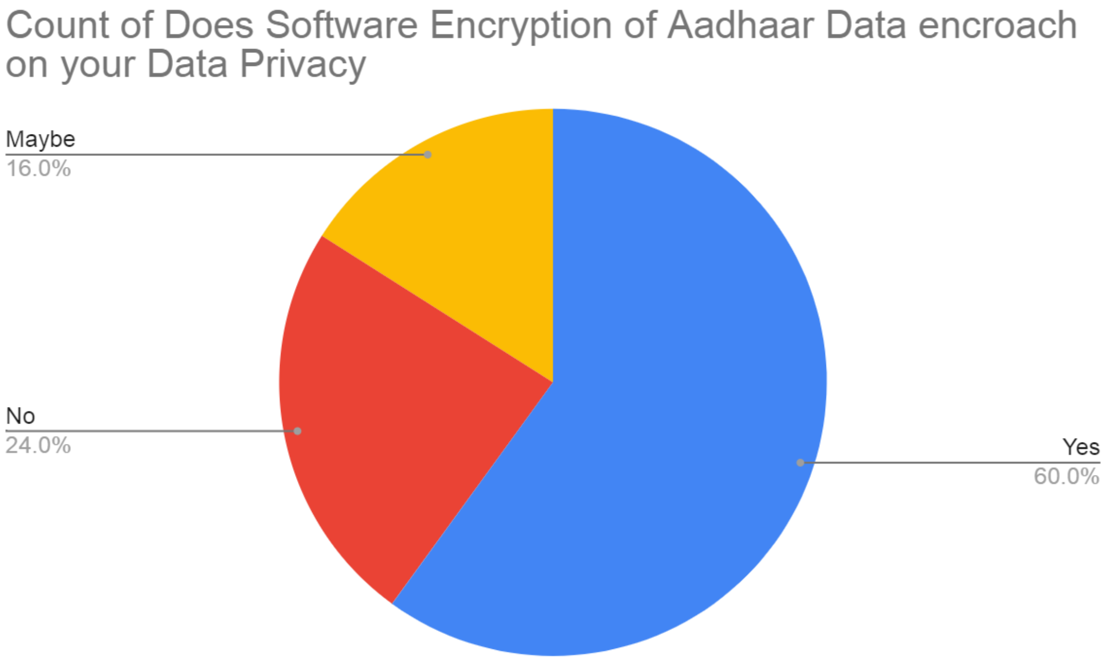
The Research Paper Discusses the Contradictory Reports on the Security and Privacy of Aadhaar Data because there has been a political occasion on which the Government Sold the Motor Vehicle Information to Private Parties and the people were not informed of it. The Driving License Data which is considered an crucial data has been subject to sale to third parties due to Bulk Data Sharing Policy and Procedure approved by the Ministry of Transport and Highways without even the people knowing about it. The Notification was issued on March,8 2019 which gave bulk data sharing to 87 Private Entities and 32 Government Entities and it was in violation of data privacy norms as the government gave the data without the consent of the concerned people.

The Research Paper finds that often the state is found in violation of data privacy because it was listening to specific person's whatsapp conservations which included Civil Society Groups, Social Activists, Student Leaders, Journalists etc through a Third Party Israeli Based Firm called NSO which was later sued by Whatsapp officials for encroachment of Data Privacy of its users and it said that the Indian Government had asked for such information and data.

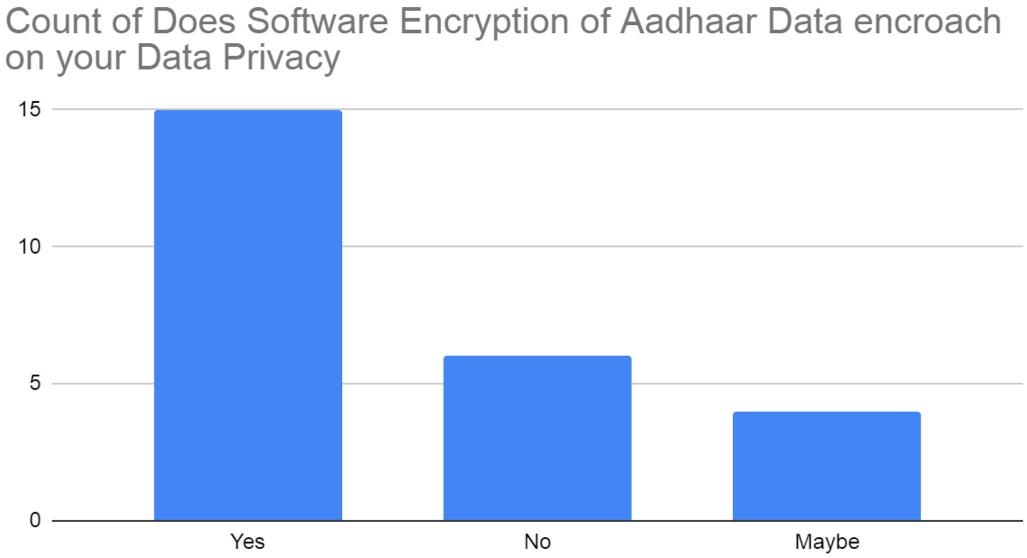
Materials and Methods

The present paper was analysed through the non-doctrinal research methodology and descriptive method of research was used. The present analysis was made through a random sampling method where the survey was taken from the common public, professionals, etc. The sample size in the present analysis is 100 samples, the independent variable in the analysis is educational qualification and the dependent variables are reliable on the statement that whether they are aware of the occurrence of social crimes and the groups provoking and promoting such illegal actions. The research tools used in the present paper such as pie diagram, bar graph and case summary were also used to analyse the study.

Analysis

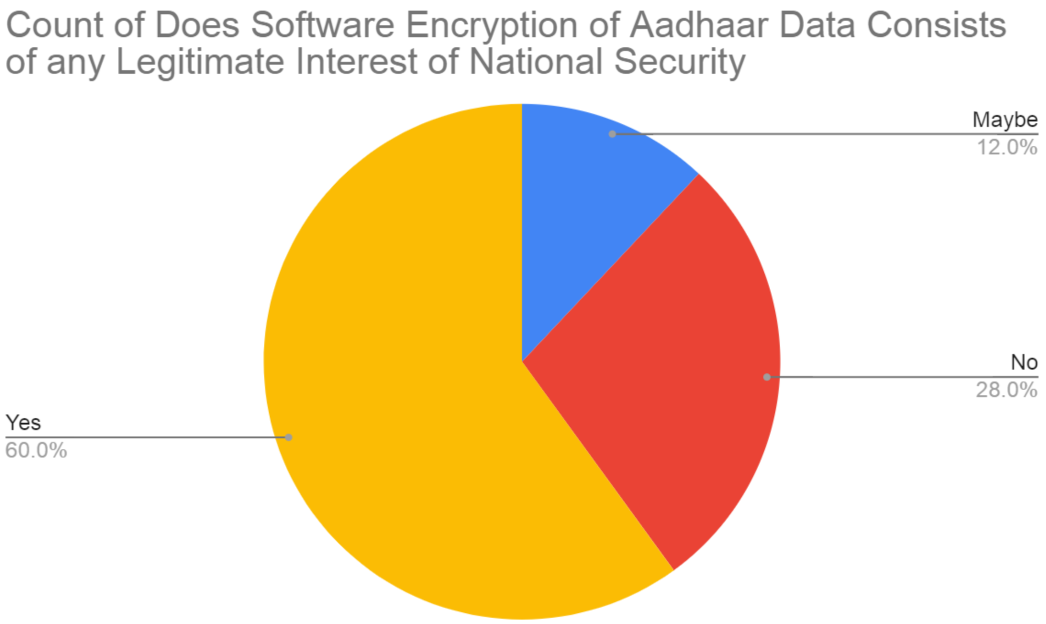


Results:- Out of the 55 Respondents interviewed for this study, 60.0% Respondents agree that Software Encryption of Aadhaar Data encroach on your Data Privacy, 24.0% Respondents interviewed for this study disagree that Software Encryption of Aadhaar Data encroach on your Data Privacy and 16.0% Respondents interviewed for this study are neutral that Software Encryption of Aadhaar Data encroach on your Data Privacy.

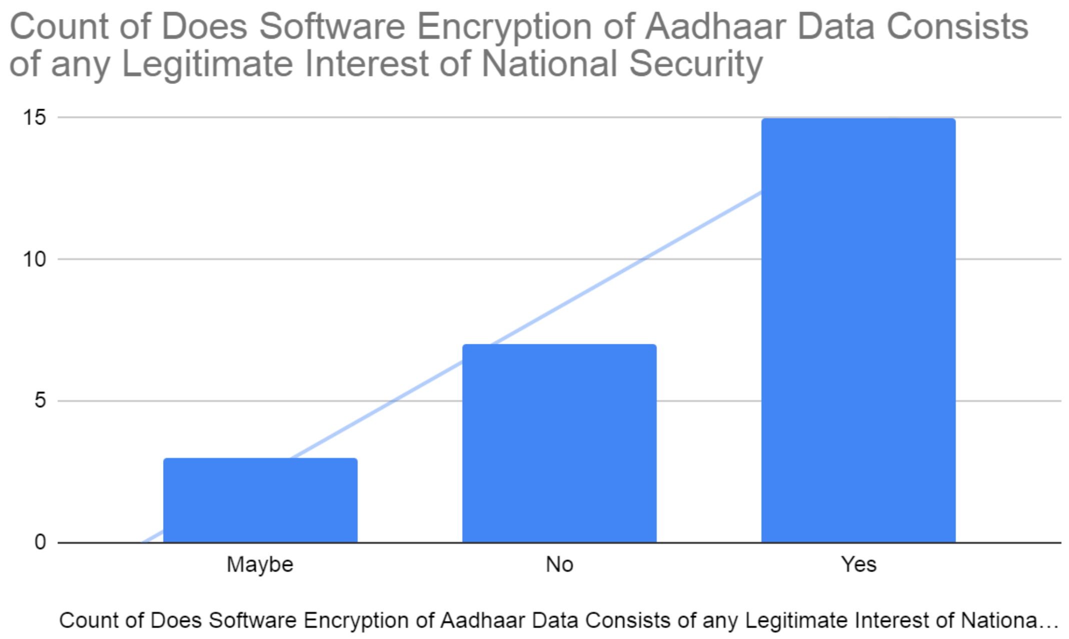


Count of Does Software Encryption of Aadhaar Data encroach on your Data Privacy

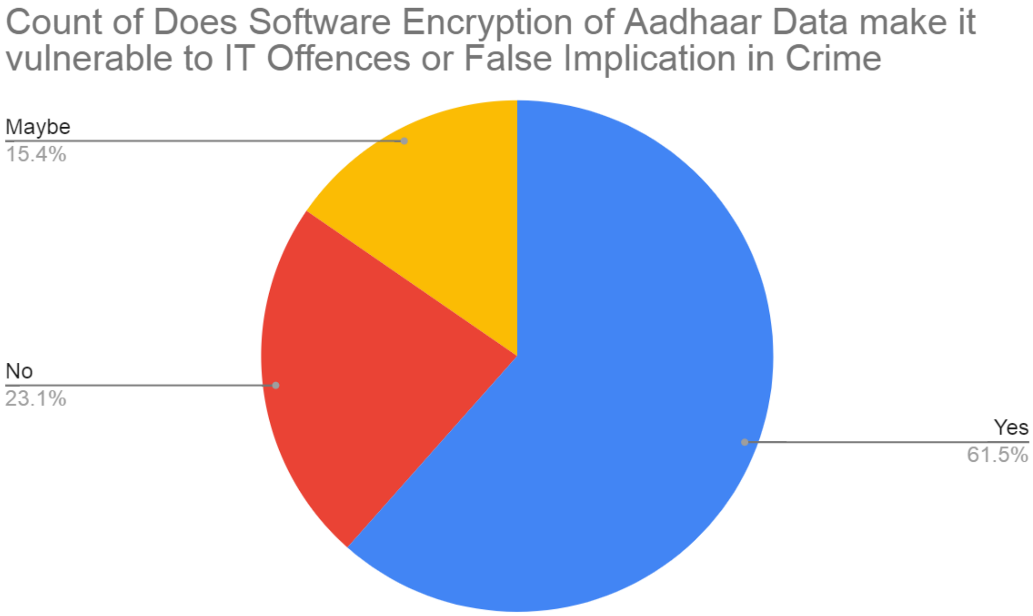
Results:- Out of the 55 Respondents interviewed for this study, 15.0% Respondents agree that Software Encryption of Aadhaar Data encroach on your Data Privacy, 6.0% Respondents interviewed for this study disagree that Software Encryption of Aadhaar Data encroach on your Data Privacy and 4.0% Respondents interviewed for this study are neutral that Software Encryption of Aadhaar Data encroach on your Data Privacy



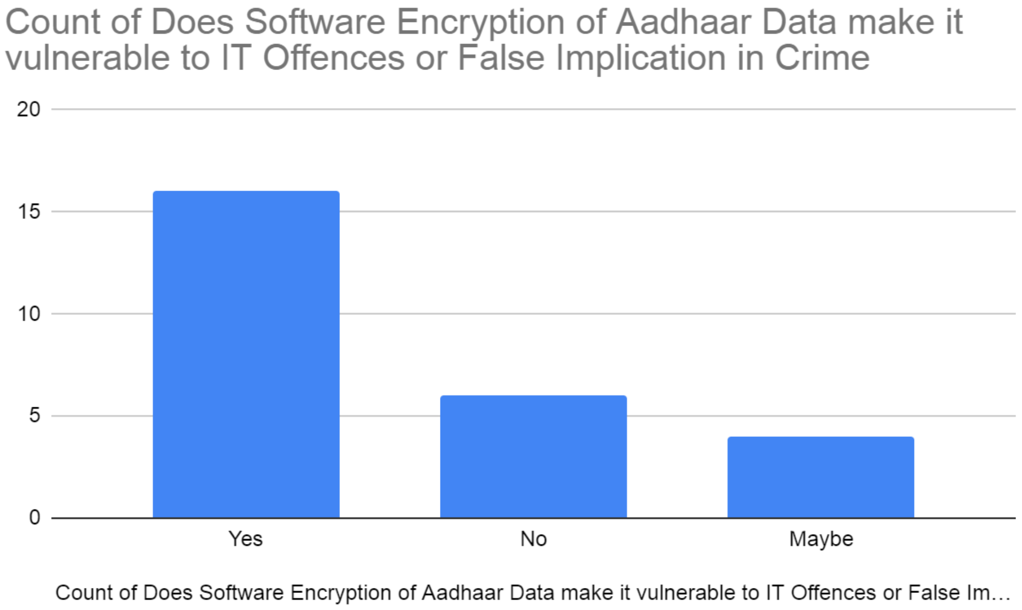
Results:- Out of the 55 Respondents interviewed for this study, 60.0% Respondents agree that Software Encryption of Aadhaar Data consists of any Legitimate Interest of National Security, 28.0% Respondents interviewed for this study disagree that Software Encryption of Aadhaar Data consists of any Legitimate Interest of National Security and 12.0% Respondents interviewed for this study are neutral that Software Encryption of Aadhaar Data consists of any Legitimate Interest of National Security.



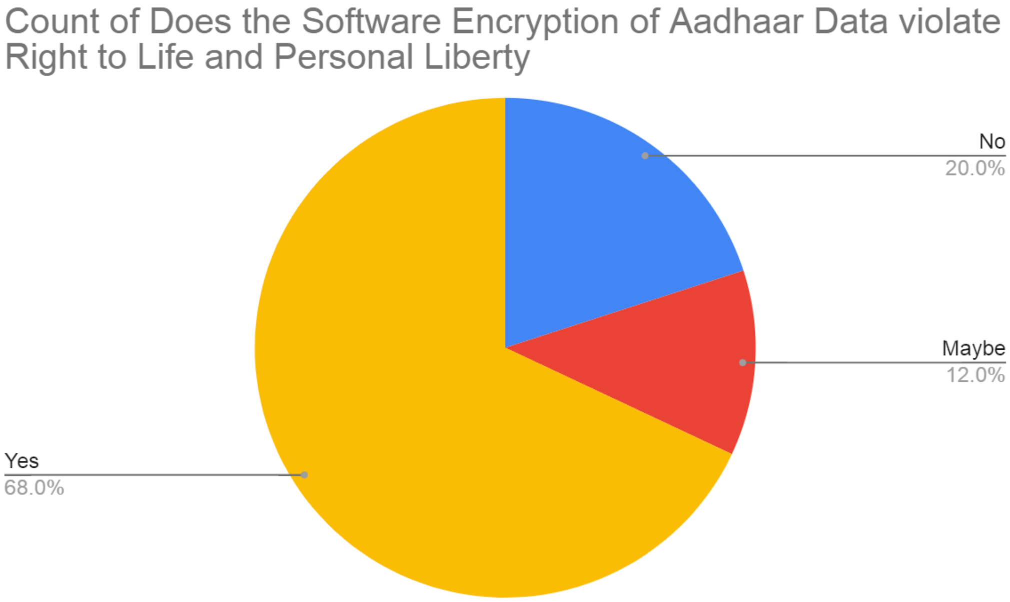
Results:- Out of the 55 Respondents interviewed for this study, 15.0% Respondents agree that Software Encryption of Aadhaar Data consists of any Legitimate Interest of National Security, 7.0% Respondents interviewed for this study disagree that Software Encryption of Aadhaar Data consists of any Legitimate Interest of National Security and 3.0% Respondents interviewed for this study are neutral that Software Encryption of Aadhaar Data consists of any Legitimate Interest of National Security.



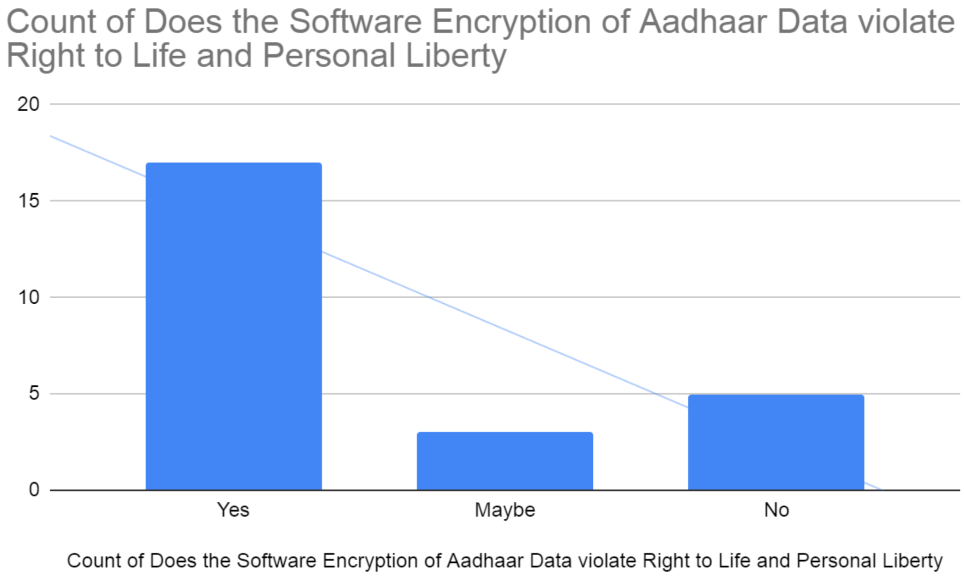
Results:- Out of the 55 Respondents interviewed for this study, 61.5% Respondents agree that Software Encryption of Aadhaar Data make it vulnerable to IT Offences or False Implication in Crime, 23.1% Respondents interviewed for this study disagree that Software Encryption of Aadhaar Data make it vulnerable to IT Offences or False Implication in Crime and 15.4% Respondents interviewed for this study are neutral that Software Encryption of Aadhaar Data make it vulnerable to IT Offences or False Implication in Crime.



Results:- Out of the 55 Respondents interviewed for this study, 16.0% Respondents agree that Software Encryption of Aadhaar Data make it vulnerable to IT Offences or False Implication in Crime, 6.0% Respondents interviewed for this study disagree that Software Encryption of Aadhaar Data make it vulnerable to IT Offences or False Implication in Crime and 4.0% Respondents interviewed for this study are neutral that Software Encryption of Aadhaar Data make it vulnerable to IT Offences or False Implication in Crime.



Results:- Out of the 55 Respondents interviewed for this study, 68.0% Respondents agree that Software Encryption of Aadhaar Data violate Right to Life and Personal Liberty, 20.0% Respondents interviewed for this study disagree that Software Encryption of Aadhaar Data violate Right to Life and Personal Liberty and 12.0% Respondents interviewed for this study are neutral that Software Encryption of Aadhaar Data violate Right to Life and Personal Liberty.



Results:- Out of the 55 Respondents interviewed for this study, 17.0% Respondents agree that Software Encryption of Aadhaar Data violate Right to Life and Personal Liberty, 5.0% Respondents interviewed for this study disagree that Software Encryption of Aadhaar Data violate Right to Life and Personal Liberty and 3.0% Respondents interviewed for this study are neutral that Software Encryption of Aadhaar Data violate Right to Life and Personal Liberty.

Discussion

AADHAR AND LEGISLATION: Firstly, The Aadhar Policy was implemented without a Legislation being passed in the Parliament which was later passed in the National Parliament and after the sensitive information's infighting within cyberspace, legislative and legal forums it caused chaos in the Public Forums among the citizens of this country whether their data was safe and secure in the digital world as this data can be misused against them for false implication in a crime, Cyber Crime and economic theft which could cause social disregard and create a disorganisation and deviation from the social freedom for awaited legal reforms and political requests for rights and cyberspace free from viruses and worms which can cause economic destruction to your economic information. Aadhar data's Misuse is also Violative of Section 66E of the Information Technology Act,2000. After the 2008 Amendment the Information Technology Act,2000 has become more outdated and not consistent with the Modern Digital

Congregation and the Punishment has to be Amended and made more stringent and Socio-Legal Requirements should be considered. Software which is used for surveillance by different countries using bugs and other tapping instruments to cause national damage to a nation's property and other infrastructure with a wrong intention can be caused. New Smart Television sold in the market with unique features such as internet connectivity can be used for violation of privacy and voyeurism. The Aadhar Act is for Subsidies and Identity whose Constitutional Validity has been challenged in the Supreme Court in the Case of **Justice K.S. Puttaswamy v/s Union of India** for Violation of Privacy and Right to Life. Aadhar Says it's not proof of citizenship but has been acquired by Refugees and Illegal Immigrants and Intruders from Neighbouring Countries. It is a Violation of privacy in the sense that it can cause hurt to Human Dignity which is a Socio-Economic Rights and Resorts to Fundamental Right. Aadhar can't be asked by CBSE and any other body which is not recognised by a Statutory Body of Law. Privacy was also discussed in the case of **M.P. Sharma v/s Satish Chandra** and **Kharak Singh v/s State of Uttar of Pradesh** but not in as varsity as of the Aadhar Case which it is famously known as. It was initially made for the welfare of the underprivileged people and to deliver the fair economic justice and applicability of government welfare schemes and social security measures to those who were deprived of those rights. It was also used to keep checks and balances over those who were running a parallel economy in the world. When it was decided to upload the details of the Aadhar Info into the UIDAI Server which was later known to leaked. It caused a sensation of fear and anxiousness that the personal data, professional data, economic data and social-economic benefits received were falling into a hacking-prone zone which could be difficult to recover.

Suggestions

- Protection of Data Privacy and Personal Liberty of an Individual is symbolism of an free society
- Further Study can be made with comparison and analysis with any other country's data protection system.

Conclusion

The Software Encryption of Aadhaar Data may sound good to the Internet Age but there are faults and legislative mistakes which ought to be repaired or amended as said in legislative language. It is an Direct Encroachment into the People's Personal Liberty and the objective of this exercise is not yet explained to the people as it can endanger any person's social or economic life because it gives a large amount of bargaining power to the person having the Aadhaar Data and it can be misused for illegal, arbitrary and malafide purposes. It should not affect the personal lives of any citizen. Section 66-E of the Information Technology Act,2000 lays the punishment for violation of privacy but how will the violator of privacy be found when the Aadhaar Data is software encrypted. The Data Protection Law has not given a Clear Vision for the Digital Empowerment and Privacy Protection of the Users. The Concept of Data Privacy can be denied if there exists an legitimate state interest and it satisfies the test of proportionality. Data Privacy is an Inherent Part of Article 21 of the Constitution and the data of a citizen can't be sold to a third party private entity without the consent of the individual. Therefore, the conclusion of the study is that the state should reconsider the legal changes to be made to protect the data privacy of the citizens and ensure that the sanctity of sensitive information provided to the state remains protected. The penalties for violation of data privacy should be framed and it should be consistent with the existing legal framework,

Acknowledgments and credits

This work is completed through the Motivation and Inspiring Thoughts given by our Faculties, Parents and the credit for this work goes to the persons who have contributed in the making of this Research Paper and collection of Research Data.

References

1. (Wilson, n.d.)
2. (Abraham and Hickok 2012)
3. (Lakhtaria et al. 2012)
4. (N.Havanurkar et al. 2015)
5. (Shanmugapriya and Kavitha 2019)
6. (J et al. 2016)

7. (Dubey and Verma 2019)
8. (Goyal and Kumar 2016)
9. (Pugazhenthi and Chitra 2019)
10. (Greenleaf 2014a)
11. (Nettleton 2014)
12. (Greenleaf 2014b)
13. (Venkataramanan and Shriram 2016)
14. (Walters, Trakman, and Zeller 2019)
15. (Matthan 2018)
16. (Singh 2019)
17. (Shaikh and Shaikh, n.d.)
18. (Anusha and A K R 2017)
19. (Dayal and Singh 2016)
20. (Kotwal, Parsheera, and Kak 2017)
21. (Rajput and Gopinath 2018)

Abraham, S., and E. Hickok. 2012. "Government Access to Private-Sector Data in India." ***International Data Privacy Law*****. https://doi.org/10.1093/idpl/ips028.**

Anusha, A. K. R. S., and A K R. 2017. "Privacy and Security Issues in Aadhaar." ***International Journal for Research in Applied Science and Engineering Technology*****. https://doi.org/10.22214/ijraset.2017.8317.**

Dayal, Mohit, and Nanhay Singh. 2016. "An Anatomization of Aadhaar Card Data Set – A Big Data Challenge." ***Procedia Computer Science*****. https://doi.org/10.1016/j.procs.2016.05.260.**

Dubey, R. K., and Ajay Verma. 2019. ***Data Protection and Privacy Implementation: India Perspective*****.**

Goyal, Gaurav, and Ravinder Kumar. 2016. ***The Right to Privacy in India: Concept and Evolution*****. Partridge Publishing.**

Greenleaf, Graham. 2014a. "India—Confusion Raj, with Outsourcing." ***Asian Data Privacy Laws*****. https://doi.org/10.1093/acprof:oso/9780199679669.003.0015.**

———. 2014b. ***Asian Data Privacy Laws: Trade & Human Rights Perspectives*****. OUP Oxford.**

J, Nitha Sagar, Department Of Information Science and Engineering, The National Institute of Engineering, Mysuru, and India. 2016. "Preserving Data Privacy without Secure Channel." ***International Journal Of Engineering And Computer Science*****. https://doi.org/10.18535/ijecs/v5i6.08.**

Kotwal, Vinod, Smriti Parsheera, and Amba Kak. 2017. "OPEN Data & Digital Identity: Lessons for Aadhaar." ***2017 ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K)*****. https://doi.org/10.23919/itu-wt.2017.8246983.**

Lakhtaria, Ritesh P., Lecturer, V. R. Godhaniya I. T. College, Porbandar, and Dhaval R. Kathiriya. 2012. "A Case Study of Electronic Government, Data Collection and Privacy Issues in India." ***International Journal of Scientific Research*****. https://doi.org/10.15373/22778179/nov2012/5.**

Matthan, Rahul. 2018. ***Privacy 3.0: Unlocking Our Data-Driven Future*****. HarperCollins.**

Nettleton, David. 2014. "Data Privacy and Privacy-Preserving Data Publishing." ***Commercial Data Mining*****. https://doi.org/10.1016/b978-0-12-416602-8.00018-2.**

N.Havanurkar, Ms Shashikala, Ms Shashikala N. Havanurkar, Department of Computer Science and Engineering, N. B. Navale Sinhgad College of Engineering, Kegaon, Solapur, India, et al. 2015. "Paradigm of Privacy Preserving Techniques in Social Network Data Publishing." ***International Journal Of Engineering And Computer Science*****. https://doi.org/10.18535/ijecs/v4i9.19.**

Pugazhenthi, A., and D. Chitra. 2019. "Data Access Control and Secured Data Sharing Approach for Health Care Data in Cloud Environment." ***Journal of Medical Systems*** **43 (8): 258.**

Rajput, Ajinkya, and K. Gopinath. 2018. "Analysis of Newer Aadhaar Privacy Models." ***Information Systems Security*****. https://doi.org/10.1007/978-3-030-05171-6_20.**

Shaikh, Dr Ahmad, and Ahmad Shaikh. n.d. "The AADHAAR Act: Is It Disturbs the Right to Privacy? A Critical Study." ***SSRN Electronic Journal*****. https://doi.org/10.2139/ssrn.3550738.**

Shanmugapriya, E., and R. Kavitha. 2019. "Efficient and Secure Privacy Analysis for Medical Big Data Using TDES and MKSVM with Access Control in Cloud." ***Journal of Medical Systems*** **43 (8): 265.**

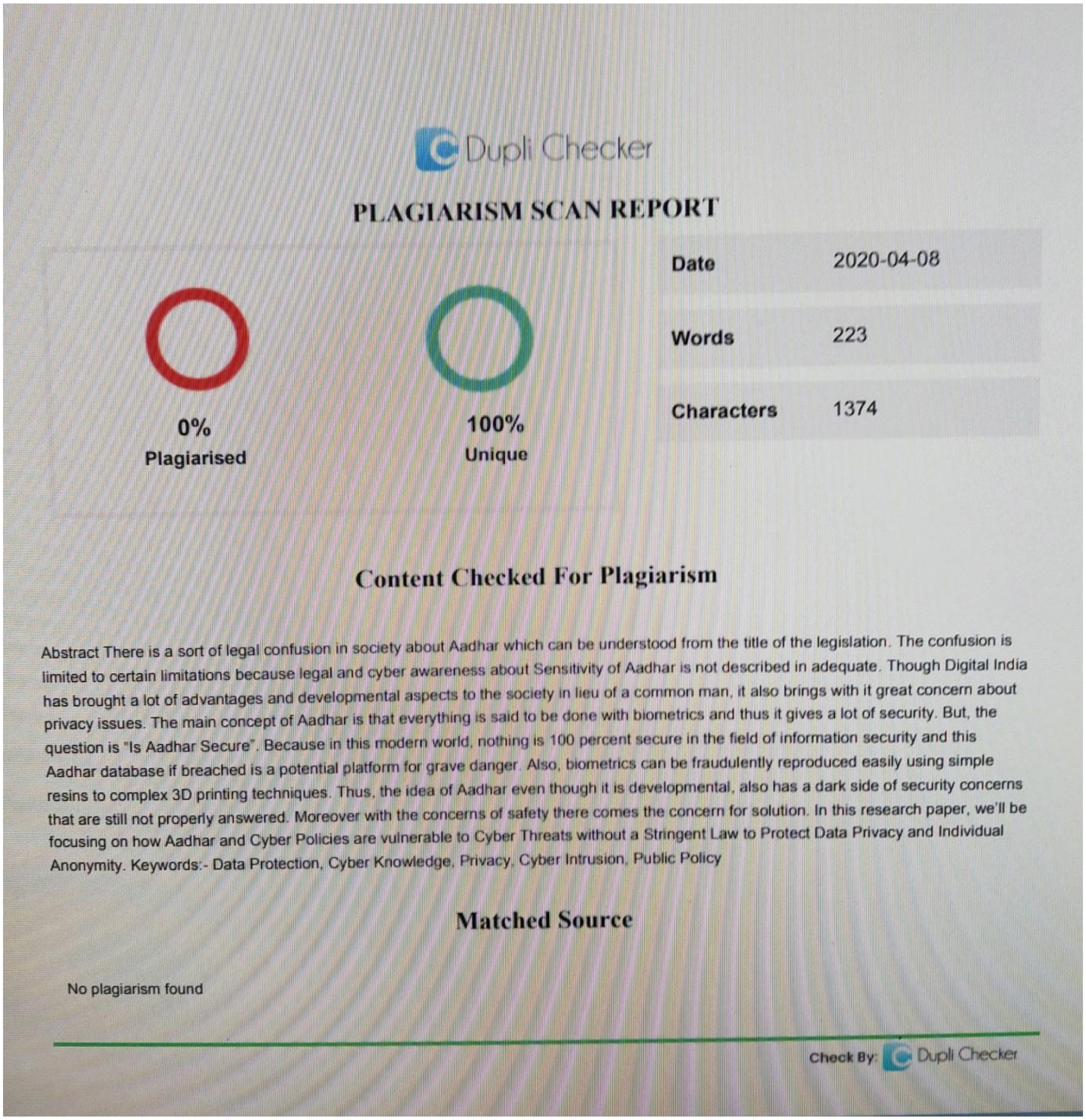
Singh, Pawan. 2019. "Aadhaar and Data Privacy: Biometric Identification and Anxieties of Recognition in India." ***Information, Communication & Society*****. https://doi.org/10.1080/1369118x.2019.1668459.**

Venkataramanan, Nataraj, and Ashwin Shriram. 2016. ***Data Privacy: Principles and Practice*****. CRC Press.**

Walters, Robert, Leon Trakman, and Bruno Zeller. 2019. ***Data Protection Law: A Comparative Analysis of Asia-Pacific and European Approaches*****. Springer Nature.**

Wilson, Benjamin. n.d. "Data Privacy in India: The Information Technology Act." ***SSRN Electronic Journal*****. https://doi.org/10.2139/ssrn.3323479.**

Plagiarism Snapshot



PLAGIARISM SCAN REPORT

Date	2020-04-08
Words	223
Characters	1374

0%
Plagiarised

100%
Unique

Content Checked For Plagiarism

Abstract There is a sort of legal confusion in society about Aadhar which can be understood from the title of the legislation. The confusion is limited to certain limitations because legal and cyber awareness about Sensitivity of Aadhar is not described in adequate. Though Digital India has brought a lot of advantages and developmental aspects to the society in lieu of a common man, it also brings with it great concern about privacy issues. The main concept of Aadhar is that everything is said to be done with biometrics and thus it gives a lot of security. But, the question is "Is Aadhar Secure". Because in this modern world, nothing is 100 percent secure in the field of information security and this Aadhar database if breached is a potential platform for grave danger. Also, biometrics can be fraudulently reproduced easily using simple resins to complex 3D printing techniques. Thus, the idea of Aadhar even though it is developmental, also has a dark side of security concerns that are still not properly answered. Moreover with the concerns of safety there comes the concern for solution. In this research paper, we'll be focusing on how Aadhar and Cyber Policies are vulnerable to Cyber Threats without a Stringent Law to Protect Data Privacy and Individual Anonymity. Keywords:- Data Protection, Cyber Knowledge, Privacy, Cyber Intrusion, Public Policy

Matched Source

No plagiarism found