खण्ड-10, अंक-1, वर्ष-2022, मु0प्र0 33-37
D.O.I.: https://doi.org/10.22445/avsp.v10i1.6
SJIF (2021) : 7.247

शोध पत्र

Application of Machine Learning and Artificial Intelligence for securing Cyber Space and the Role of Government Organization

Deepayan Malaviya
Jindal Global Law School
O.P. Jindal Global University, Sonipat-131 001, Haryana
dmalaviya@jgu.edu.in

Received: 08-08-2022, Accepted: 05-09-2022

Abstract-Digitization is the talk of the day and everything everywhere is being digitized. On one hand digitization presents immense importance from the view point of convenience but at the same time it raises pertinent questions regarding security. The paper presents a discussion on the various aspects relating to cyber space, cyber security, cyber law and the step by government to make the Indian cyber space safe and secure. The paper also takes into account data which shows the trends of cyber-attacks and compares the nature of attacks with the steps taken by the government to curtail such attacks in the future. Towards the end, the paper provides solutions for the better development of cyber security protocols in India.

Key words- Digitization, Cyber Security, Cyber Law, Artificial Intelligence, Machine Learning, Internet

साइबर स्पेस को सुरक्षित रखने में मशीन अधिगम एवं कृत्रिम बुद्धि का प्रयोग और इसमें सरकारी संगठनों की भूमिका

दीपायन मालवीय
जिंदल ग्लोबल लॉ स्कूल
ओ0 पी0 जिंदल ग्लोबल यूनिवर्सिटी, सोनीपत–131 001, हरयाणा, भारत
dmalaviya@jgu.edu.in

सार– आज के समय में डिजीकरण बहुचर्चित है। यह इसलिए है क्योंकि डिजीकरण चीजों को बहुत आसान और सुविधाजनक बना देता है। सुविधाजनक और आसान बनाने के साथ–साथ डिजीकरण सुरक्षा से सम्बंधित सवाल भी चर्चा में सम्मिलित करता है। इस लेख के माध्यम से साइबर स्पेस, साइबर सुरक्षा साइबर विधि अथवा सरकारी नीतियों को बारीकी से समझा जायेगा और ये जानने का प्रयास किया जायेगा कि क्या इन सब से भारत की साइबर स्पेस सुरक्षित हो रही है या नहीं ? साथ ही बीते कुछ सालो में कितने साइबर हमले हुए हैं और सरकारी नीतिओं का इन हमलों पर क्या प्रभाव पड़ा है ये भी समझने का प्रयास किया जायेगा। अंत में भारत की साइबर स्पेस को और सुरक्षित कैसे करा जाय, इसके उपायों पर भी विचार किया जायेगा।

बीज शब्द– डिजीकरण, साइबर सुरक्षा, साइबर विधि, कृत्रिम बुद्धिमत्ता, मशीन अधिगम, इंटरनेट

1. **परिचय**– विश्व का भविष्य डिजिटल होने वाला है और आने वाले समय में इस डिजीकरण की गति और भी बढ़ने वाली है। डिजीकरण के कारण उपभोक्ता को जब जो वस्तु चाहिए वह वस्तु उसे उसी क्षण मिलने की सम्भावना भी बढ़ गई है। इसके चलते इंटरनेट ऑफ थिंग्स (आई.ओ.टी.) की अवधारणा की उत्पत्ति एवं विकास हुआ है। सरल शब्दों में कहा जाय तो आई.ओ.टी का अर्थ यह है की वह सभी वस्तुएं जिनमें विभिन्न प्रकार के सेंसर अतः सॉफ्टवेयर हैं; वह वस्तुए इंटरनेट के माध्यम से एक दुसरे से जुडी हुई हैं। यह उपकरण घरेलू हो सकते हैं अतः औद्योगिक भी हो सकते हैं। बीते युग के विपरीत अब डाटा पेपर पर नहीं अपितु सर्वर पर संगृहीत करा जाता है। इससे कई फायदे भी हैं और कई नुकसान भी। एक ओर डाटा सुलभ हो गया है तथा दूसरी ओर डाटा को चुराना और हेराफेरी करना भी सरल हो गया है।

जैसे कि अपने घरों में हम लोग मूल्यवान वस्तुओं को ताले–चाभी से सुरक्षित रखते हैं ठीक वैसे ही सर्वर पर स्थित डाटा की सुरक्षा भी एन्क्रिप्शन, पासवर्ड इत्यादि जैसी तकनीकों से सुरक्षित की जाती है। परन्तु डिजीकरण के अतिशीघ्र होने से सुरक्षा एक कदम पीछे छूट गई है। आंकड़े बताते है कि २०२१ में विश्व में सबसे अधिक साइबर हमले एशिया में हुए और चौका देने वाली बात यह है की एशिया में होने वाले साइबर हमले के देशों में भारत तीसरे स्थान पर आता है।[1]

अब क्योंकि प्रत्येक डिजिटली वस्तु एक दुसरे से इंटरनेट के माध्यम से जुडी हुई है तो साइबर हमले से होने वाली हानि की सम्भावना बहुत बढ़ जाती है और इसी लिए साइबर सुरक्षा और भी अधिक महत्वपूर्ण हो जाती है।

2. **साइबर सुरक्षा क्या होती है ?** सरल शब्दों में कहा जाय तो साइबर सुरक्षा वो सुरक्षा है जिससे कि साइबर हमले रोके जा सकते हैं, या उनके नकारात्मक प्रभाव को कम किया जा सकता है। साइबर हमले के माध्यम से एक धोखेबाज/साइबर अपराधी प्रयोक्ता के नेटवर्क को बाधित कर सकता है। संरचनात्मक रूप से अभिकल्पित परिकलित हेराफेरी कर कंप्यूटर नेटवर्क को नष्ट किया जा सकता है जिसके कारण पूरे संस्थान को आर्थिक नुकसान उठाना पढ़ सकता है। साइबर सुरक्षा का एक ही उद्देश्य है और वो उद्देश्य है कि उपर्युक्त स्थित नुकसान से संस्थानों और व्यक्ति को बचाना।

जैसा की उपर्युक्त अनुच्छेद में कहा गया है की डिजीकरण बहुत तेजी से हुआ है और डाटा को सुरक्षित रखना मानवीय रूप से संभव नहीं है, इसके लिए कृत्रिम बुद्धिमत्ता का प्रयोग किया गया है। ठीक वैसे ही जैसे सुरक्षा प्रणाली को कृत्रिम बुद्धिमत्ता का प्रयोग कर के मजबूत बनाया गया है। उसी प्रकार अपराधियों ने भी कृत्रिम बुद्धिमत्ता का प्रयोग कर के अपने हमलों को सुधारा है।[२]

3. **कृत्रिम बुद्धिमत्ता, मशीन अधिगम एवं साइबर सुरक्षा पर इनके प्रभाव**– एक सामान्य इंसान के लिए कृत्रिम बुद्धिमत्ता केवल एक रोबोट की कल्पना हो सकती है परन्तु तकनीकी तौर पर कहा जाय तो कृत्रिम बुद्धिमत्ता इससे कही अधिक है। जे मैककार्थी, एम0 एल0 मिंस्की, एन0 रोचेस्टर, और सी0 ई0 शैनन की परियोजना कृत्रिम बुद्धिमत्ता को बड़े अच्छे से परिभाषित करता है।[३]साथ ही एलन टर्निंग, कृत्रिम बुद्धिमत्ता के संस्थापक, ने कृत्रिम बुद्धिमत्ता की बुनियाद १९५० में ही "क्या मशीन सोच सकती है?" सवाल पूछ कर कर दी थी।[४] सामान्यता कृत्रिम बुद्धिमत्ता एक ऐसी प्रौद्योगिकी है जिसमें मानव सोच हो सकती है या वह प्रौद्योगिकी है जो कुछ भी सीखती है उसके आधार पर परिणाम उत्पन्न कर सकती है। यह भी कहा जा सकता है की कृत्रिम बुद्धिमत्ता मानवीय बुद्धि की नकल है जो की मशीन द्वारा की जाती है। कृत्रिम बुद्धिमत्ता की तुलना एक स्व–सीख एल्गोरिदम से भी की जा सकती है।

मशीन अधिगम भी कृत्रिम बुद्धिमत्ता का एक प्रारूप है। मोटे तौर पर कहे तो कृत्रिम बुद्धिमत्ता से सॉफ्टवेयर बुद्धिमान प्रतीत होता है परन्तु वो सॉफ्टवेयर जिस डाटा का उपयोग कर के बुद्धिमान होता है उस तकनीक को मशीन अधिगम कहा जाता है। मशीन अधिगम में बहुत सारा डाटा सॉफ्टवेयर द्वारा संसाधित किया जाता है, और इसी संसाधन से मशीन अपने आप को सिखाती है। यह कहना गलत नहीं होगा कि मशीन अधिगम से सॉफ्टवेयर परिशिष्ट होता है और बुद्धिमत्ता के पथ पर अग्रसर होता है।[५] उद्धरण के तौर पर इसे इस तरह समझा जा सकता है कि एक मशीन को बता दिया गया है की उसे बिंदु 'आ' से बिंदु 'स' तक जाना है साथ ही उस मशीन को डाटा दिया जाता है जिससे कि वह मशीन बुद्धिमत्ता के पथ पर अग्रसर हो सके, इसके साथ उसके सॉफ्टवेयर को स्वयं सीखने की क्षमता भी प्रदान की जाती है। परिणाम स्वरुप वह मशीन पुनरूक्तियाँ करती है और बिंदु 'आ' से बिंदु 'स' तक पहुँचने का सबसे सीधा सरल और छोटा रास्ता स्वयं प्राप्त कर लेती है।

डिजीकरण हेतु सभी वस्तुएं डिजिटल प्रारूप में बदली जा रही है। क्योंकि संगठनों को तरक्की करनी है और क्योंकि तरक्की के लिए इंटरनेट अहम् है तो सभी संगठन डिजिटल रूप से इंटरनेट से जुड़े हुए है। और तो और अधिकतर संगठनों का डाटा ऑनलाइन सर्वर में स्थित है। समृद्धि के लिए कृत्रिम बुद्धिमत्ता एवं मशीन अधिगम भी आवश्यक हो जाता है। आज के समय में डाटा इतना अधिक हो चुका है कि इंसान के बस में उसे नियंत्रित और प्राकृत करना असंभव हो गया है, इसलिए इंसान को कृत्रिम बुद्धिमत्ता एवं मशीन अधिगम की अधिक आवशकता पड़ती है। साइबर स्पेस के क्षेत्र में भी कुछ ऐसा है। वो समय आ चुका है जब नेटवर्क की रक्षा करने वाले और नेटवर्क को हानि पहुंचाने वाले दोनों ही कृत्रिम बुद्धिमत्ता एवं मशीन अधिगम का उपयोग कर के ऐसा कंप्यूटर सॉफ्टवेयर बना रहे है जो कि स्वयं ही किसी सर्वर को भेद कर संवेदनशील डाटा को अतिसंवेदनशील बना सकते हैं और इससे उपभोक्ता को हानि पहुंच सकती है।

अब क्योंकि नेटवर्क के हमलावर और रक्षक दोनों ही इन तकनीकों का इस्तेमाल कर रहे हैं तो 'लाभ के संतुलन' को निर्धारित करना कठिन हो जाता है।[६] ये निर्धारित करना और भी कठिन हो जाता है क्योंकि ये तकनीके मानव पर्यवेक्षण के बिना ही कार्य करती हैं और कई बार ऐसा भी होता है कि कृत्रिम बुद्धिमत्ता एवं मशीन अधिगम के मिश्रण का परिणाम सोर्स कोड पर पड़ता है और सोर्स कोड बदल जाता है जो की मूल सोर्स कोड से अलग होता है। ऐसे में कहा जा सकता है कि मशीन ने मानवीय बुद्धि को पीछे छोड़ दिया है। इस परिदृश्य में होने वाली हानि का उत्तरदायी कौन होगा यह निर्धारित करना लगभग असंभव हो जाता है।

जैसे हर सिक्के के दो पहलू होते हैं वैसे ही कृत्रिम बुद्धिमत्ता एवं मशीन अधिगाम के भी दो पहलू हैं। अभी तक हमने इसके दुष्प्रभाव के बारे में बात की है और अब हम इसके लाभ की भी बात करेंगे। जैसा की उपर्युक्त अनुच्छेदों में कहा गया है कि इन दोनों तकनीकों के प्रयोग से साइबर स्पेस की सुरक्षा को भेदा जा सकता है ठीक उसी तरह इन तकनीकों का प्रयोग साइबर स्पेस को सुरक्षित बनाने के लिए भी किया जा सकता है। मशीनी अधिगम में एक तकनीक होती है रिग्रेशन और इस तकनीक का उपयोग कर के साइबर रक्षक किसी भी साइबर हमले का पूर्वानुमान लगा सकते हैं।[७]

4. **भारत में साइबर सुरक्षा के बदलते आयाम**– साइबर सुरक्षा अथवा सुरक्षा की संकल्पना पिछले दशक में बहुत बदली है। पहले एंटी वायरस सॉफ्टवेयर से सिस्टम को सुरक्षित करा जा सकता था परन्तु अब ऐसा नहीं है। साइबर सुरक्षा घटनाएं जो कि सन् २०१० में मात्र १०३१५ थी वह बढ़कर सन् २०२१ में १४ लाख से भी अधिक हो गई। इससे पता चलता है कि साइबर सुरक्षा एक राष्ट्र के लिए कितनी महत्वपूर्ण हैं। इसके अतिरिक्त भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया टीम ने २०२१ में ६१८ सुरक्षा चेतावनियां जारी की। सन् २०२१ में २ लाख से ज्यादा दुर्भावनापूर्ण कोड पकड़े गई आदि। **तालिका–१** इन घटनाओं के बारे में विस्तृत रूप से व्याख्या करती है तथा **तालिका–२** सुरक्षा घटनाओं का विवरण देती है।

4.1 **तालिका–१- प्रबंधित घटनाएं**[8]

गतिविधियां	सन्२०२१
सुरक्षा घटनाओं का निवारण	१४२८०६
सुरक्षाछिद्र नोट्स प्रकाशित	३६०
प्रकाशित परामर्श	५२
सुरक्षा अलर्ट जारी	६१८
प्रशिक्षण आयोजित	१६
साइबर सुरक्षा मॉक ड्रिल	
राष्ट्रीय अभ्यास/व्यायाम	६
अंतर्राष्ट्रीय अभ्यास/ अभ्यास	७

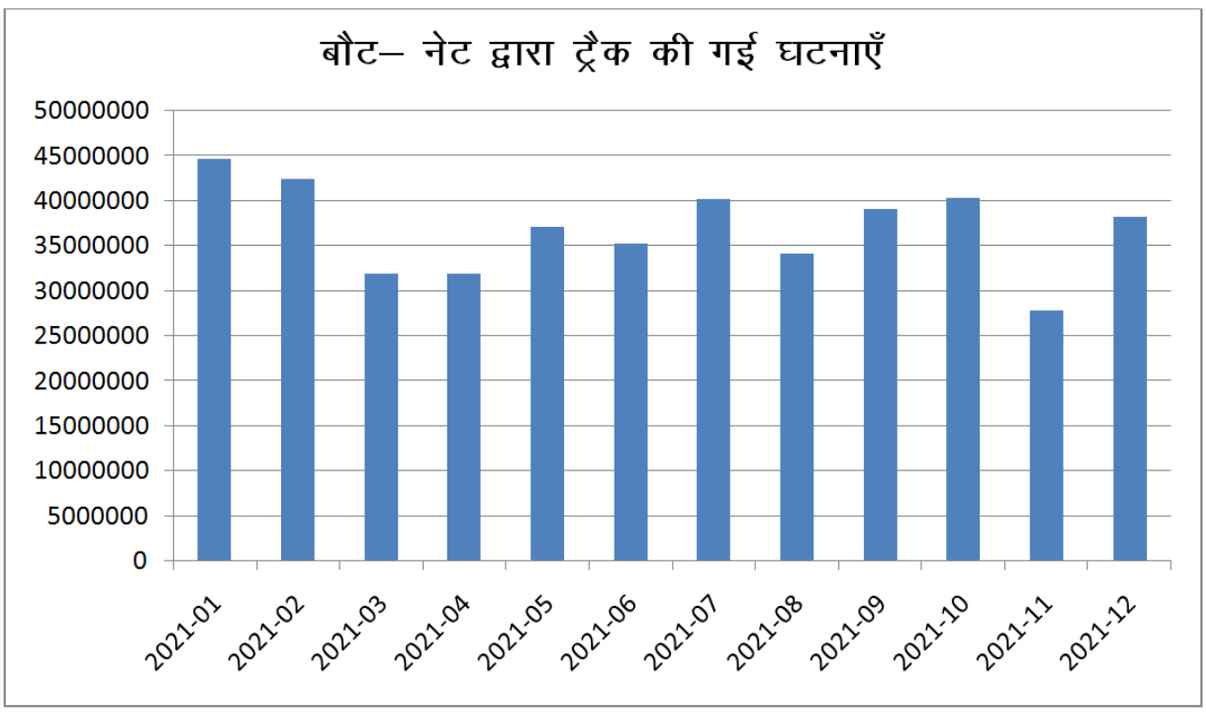
4.2 **तालिका–२ -सुरक्षा घटनाओं का विवरण**[9]

सुरक्षा घटनाएं	सन् २०२१
फिशिंग	५२३
अनधिकृत नेटवर्क स्कैनिंग/जाँच	४३२०५७
असुरक्षित सेवा	७२८२७६
वायरस/ दुर्भावनापूर्ण कोड	२०६११०
वेबसाइट विरूपण	२७४०८
वेबसाइट घुसपैठ और मालवेयर प्रचारण	१४८६
अन्य	३६४६
कुल	**१४०२८०६**

नई तकनीकों के विकास के कारण भारत के बदलते खतरे के परिदृश्य को प्रोत्साहन प्राप्त हो रहा है। राष्ट्रीय सॉफ्टवेयर और सेवा कंपनियों के संघ ने रिपोर्ट किया है कि भारत २०२० तक इंटरनेट ऑफ थिंग्स के बाजार का २०% हिस्से पर अपना हक जमाने की इच्छा रखता है। इसके चलते व्यवसाय साइबर सुरक्षा के प्रति संवेदनशील हो रहे हैं।[10]

साथ ही सरकार के भी कई कदम हैं जो कि साइबर स्पेस को सुरक्षित करने के लिए उठाए गए हैं। इनमें से सबसे पहला कदम है कंप्यूटर आपातकालीन प्रतिक्रिया टीम को स्थापित करना। ये टीम साइबर घटनाओ के प्रबांधन के लिए एक नोडल एजेंसी है। इस एजेंसी के पास आधुनिक उपकरण हैं जिनकी सहायता से ये खतरों को नियंत्रित करती है। इसके साथ ही भारत के पासएक संकट प्रबंधन योजना है जिससे कि साइबर हमला होने पर मानक प्रचालन प्रक्रियाएं स्वयं संचालित हो जाती है। इसका लाभ ये है कि बड़े पैमाने पर व्यवधान नहीं होता है और घटना या हमला निरस्त्र हो जाता है। २०१७ में भारत सरकार ने साइबर स्वच्छता केंद्र की स्थापना की थी। इस केंद्र का मूल उद्देश्य बौट–नेट संक्रमण को पहचान कर नष्ट करना है। आगे बौट–नेट के संक्रमण न हो इसलिए ये केंद्र अंतिम प्रयोक्ता के नेटवर्क सिस्टम को सुरक्षित भी करता है। **तालिका–३** इस केंद्र के बारे में विस्तृत रूप से सूचना देती है।[11]

4. तालिका ३- बौट–नेट द्वारा ट्रैक की गई घटनाएँ[12]



इनफॉर्मेशन टेक्नोलॉजी अधिनियम, २००० के अनुच्छेद ७०अ के तहत एक विशेष अभिकरण की मांग करी जाती है जो कि क्रांतिक अवसंरचना को साइबर हमलों से सुरक्षित रखे। इस अधिनियम के चलते राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केन्द्रकी स्थापना की गई। इस केंद्र के अलावा राष्ट्रीय साइबर समन्वय केंद्र की भी स्थापना की गई है। यह केंद्र भारत में ई–निगरानी रखने वाली राष्ट्रीय सुरक्षा एजेंसी है। यह एजेंसी मुख्य रूप से साइबर अपराध और साइबर आतंकवाद को कम करने के लिए कार्य करती है।

इन तकनीकों के अलावा साइबर फोरेंसिक, सी.वी.ई. क्रमांकन प्राधिकरण एवं ऐसे सिस्टम बनाये गये हैं जो कि साइबर स्पेस में होने वाले खतरों को पहचान कर उन्हें दूसरी प्रणालियों तक पहुंचा देते हैं। इन सब तकनीकों से यह फायदा होता है कि भारत की साइबर स्पेस सुरक्षित रहती है।

5. **भारतीय साइबर सुरक्षा एवं वित्तीय सहायता एवं समाप्ति**– २०१५ से २०२१ तक भारत सरकार ने साइबर सुरक्षा के लिए आवंटन बढ़ाया है। २०१५–१६ में आवंटन मात्र ८५ करोड़ था जो कि आज बढ़ कर ४१६ करोड़ हो गया है। परन्तु इसका ये तात्पर्य नहीं है कि भारतीय साइबर सुरक्षा प्रणाली बेहतर हो गई है। इसका तात्पर्य ये है कि बढ़ते खतरों के साथ भारत देश कदम से कदम मिला कर चल रहा है या चलने की कोशिश कर रहा है।[13]

6. **निष्कर्ष**– कोरोना के पश्चात् व्यवसाय और अन्य कार्य ऑनलाइन हो गए और इसने इंटरनेट को और भी अधिक महत्वपूर्ण बना दिया जिसके चलते साइबर स्पेस को सुरक्षित रखना आवश्यक हो गया क्योंकि अपराध भी इंटरनेट के माध्यम से होने लगे। चूँकि भारत अभी विकासशील देश है तो इस बात की सम्भावना बढ़ जाती है कि उसके पास पूर्ण रूप से विकसित देशों की तुलना में तकनीकी ज्ञान कम होगा। ये होने के कारण भारत की साइबर स्पेस साइबर हमलों के प्रति संवेदनशील साबित हो सकती है। इस परिस्थिति में बुद्धिमत्ता इसी में है कि पूर्णतः विकसित देशों से सहयोग लिया जाय और साथ मिल कर इन साइबर हमलों से बचने की अत्याधुनिक तकनीकों पर काम किया जाय।

References

1. IANS, Cyber attacks: India among top 3 most-affected nations in Asia in 2021, Business Standard, 2021, https://www.business-standard.com/article/international/cyber -attacks-india-among-top-3-most-affected-

nations-in-asia-in-2021-122022400945_1.html.
2. Zaidi, Khadeeja (2021)Artificial intelligence and cyber law, https://blog.ipleaders.in/artificial-intelligence-cyber-law/ (last visited Jun 8, 2022).
3. McCarthy, J. et al. (1955) A PROPOSAL FOR THE DARTMOUTH SUMMER RESEARCH PROJECT ON ARTIFICIAL INTELLIGENCE, (1955), http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf.
4. A M Turning, Computing Machinery and Intelligence, LIX Mind 43340 (1950).
5. Kristin Burnham, Artificial Intelligence vs. Machine Learning: Whats the Difference?, Artificial Intelligence vs. Machine Learning: Whats the Difference?(2020), https://www.northeastern.edu/graduate/blog/artificial-intelligence-vs-machine-learning-whats-the-difference/ (last visited Jun 8, 2022).
6. Future Series: Cybersecurity, emerging technology and systemic risk, 159 (2020), https://www3.weforum.org/docs/WEF_Future_Series_Cybersecurity_emerging_technology_and_systemic_risk_2020.pdf.
7. Julien Maury, AI & ML Cybersecurity: The Latest Battleground for Attackers & Defenders, (2022), https://www.esecurityplanet.com/threats/ai-ml-cybersecurity/ (last visited Jul 8, 2022).
8. Indian Computer emergency Response Team (CERT-In), CERT-In Annual Report, 122 (2022), https://cert-in.org.in/.
9. Id. at 7.
10. Deloitte, AN OVERVIEW OF THE CYBER-SECURITY INDUSTRY IN INDIA, 114 (2018), https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-deloitte-itsa-pov-noexp.pdf (last visited Aug 8, 2022).
11. Indian Computer emergency Response Team (CERT-In), supra note 8 at 8.
12. Id. at 12.
13. Shekhar, Snehanshu (2021)Cyber attacks rising in India, CERT-In alerts to over 700 entities: Govt in Lok Sabha, India Today, https://www.indiatoday.in/india/story/cyber-attacks-rising-in-india-cert-in-alerts-to-over-700-entities-govt-in-lok-sabha-1833783-2021-07-28.