ಸುವಿಜ್ಞ सुविज्ञ

तकनीकी अंक - 3

वर्ष 2023

वसुधैव कुटुम्बकम्

कृत्रिम ज्ञान तथा रोबोटिकी केंद्र, बेंगलूरु

सुविज्ञ तकनीकी अंक – 3

कृत्रिम ज्ञान तथा रोबोटिकी केन्द्र

वर्ष 2023

संपादकीय समिति

डॉ. ऋतुराज कुमार
उत्कृष्ट वैज्ञानिक एवं निदेशक
अध्यक्ष, राजभाषा कार्यान्वयन समिति

संपादक मंडल

श्रीमती टी आर उषा कुमारी, वैज्ञानिक 'एफ'
उपाध्यक्षा, राजभाषा कार्यान्वयन समिति
डॉ. एस.एन. महेश, सहायक निदेशक (राजभाषा)
श्री अभिजीत पाण्डेय, कनिष्ठ अनुवाद अधिकारी

सुविज्ञ तकनीकी अंक – 3

सुविज्ञ

तकनीकी अंक-3

कृत्रिम ज्ञान तथा रोबोटिकी केन्द्र

अनुक्रमणिका

तकनीकी खंड

डॉ समिर वी कामत
सचिव, रक्षा अनुसंधान तथा विकास विभाग
एवं
अध्यक्ष, डीआरडीओ
Dr. Samir V. Kamat
Secretary, Department of Defence R&D
&
Chairman, DRDO

सत्यमेव जयते

स्वच्छ भारत
एक कदम स्वच्छता की ओर

भारत सरकार, रक्षा मंत्रालय
रक्षा अनुसंधान तथा विकास संगठन
र.अ.वि.सं. मुख्यालय, डी.आर.डी.ओ. भवन
राजाजी मार्ग, नई दिल्ली – 110 011
Government of India, Ministry of Defence
Defence Research and Development Organisation
DRDO Bhawan, Rajaji Marg, New Delhi - 110 011

संदेश

मुझे यह जानकर अपार हर्ष का अनुभव हो रहा है कि **कृत्रिम ज्ञान तथा रोबोटिकी केंद्र (केयर), बेंगलुरु** अपनी वार्षिक हिन्दी गृह पत्रिका '**सुविज्ञ**' के तृतीय तकनीकी अंक का प्रकाशन कर रहा है।

भारत जैसे विविधता वाले देश में अनेकों भाषाएं बोली जाती हैं और इन सबके बीच हिंदी ही एक ऐसी भाषा है, जो देश में संपर्क भाषा के रूप में उभरी है। हिंदी भाषा में ऐसी तकनीकी पत्रिका का प्रकाशन वास्तव में राजभाषा हिंदी की तकनीकी क्षेत्र में हो रहे उत्तरोत्तर विकास को दर्शाता है।

मुझे विश्वास है कि हिन्दी पत्रिका '**सुविज्ञ**' के इस तकनीकी अंक में वैज्ञानिक एवं तकनीकी लेखों के समावेश से यह पत्रिका पाठकों के विभिन्न वर्गों के बीच लोकप्रिय सिद्ध होगी।

मैं इस अवसर पर केंद्र के निदेशक सहित '**सुविज्ञ**' के तकनीकी अंक के प्रकाशन से जुड़े समस्त अधिकारियों एवं कर्मचारियों को उनके इस प्रयास के लिए बधाई देता हूँ और पत्रिका के सफल प्रकाशन की कामना करता हूँ।

समिर कामत

(डॉ समिर वी कामत)

सुमा वर्गीस
वि.वै. एवं महानिदेशक
(एम ई डी एवं कम्प्यूटेशनल सिस्टम)

Suma Varughese
DS and Director General
(MED & CoS)

सत्यमेव जयते

स्वच्छ भारत
एक कदम स्वच्छता की ओर

भारत सरकार, रक्षा मंत्रालय
रक्षा अनुसंधान तथा विकास संगठन
र.अ.वि.सं. मुख्यालय, डी.आर.डी.ओ. भवन
राजाजी मार्ग, नई दिल्ली – 110 011

Government of India, Ministry of Defence
Defence Research and Development Organisation
DRDO Hqrs., DRDO Bhawan
Rajaji Marg, New Delhi - 110 011

संदेश

यह हर्ष का विषय है कि **कृत्रिम ज्ञान तथा रोबोटिकी केंद्र (केयर), बेंगलुरु** विगत वर्षों की भांति इस वर्ष भी अपनी वार्षिक हिन्दी गृह पत्रिका '**सुविज्ञ**' के तृतीय तकनीकी अंक का प्रकाशन करने जा रहा है।

आशा है कि '**सुविज्ञ**' के इस तकनीकी अंक में ज्ञानवर्धक लेख प्रकाशित होंगे, जिससे राजभाषा हिंदी द्वारा हिंदी भाषी लोगों तक तकनीकी संबंधी नवीन एवं अद्यतनित सूचना पहुंचेगी।

इस विशिष्ट तकनीकी अंक के प्रकाशन से विभिन्न वैज्ञानिकों, अधिकारियों तथा कर्मचारियों को हिंदी में अपने लेख तैयार करने की प्रेरणा मिली है। मुझे पूर्ण विश्वास है कि '**सुविज्ञ**' का यह तकनीकी अंक भविष्य में भी इसी प्रकार से विभिन्न अधिकारियों तथा कर्मचारियों के लिए प्रेरणास्रोत बना रहेगा।

मैं इस सफल प्रयास के लिए केन्द्र के निदेशक के साथ ही तकनीकी अंक के प्रकाशन से जुड़े समस्त अधिकारियों एवं कर्मचारियों को हार्दिक बधाई देती हूं तथा आशा करती हूं कि भविष्य में भी इस प्रकार के उपयोगी अंक नियमित रूप से प्रकाशित होते रहेंगे ।

सुमा वर्गीस

(सुमा वर्गीस)

पुरुषोत्तम बेज
उ.वै. एवं महानिदेशक (आर एण्ड एम)

Purusottam Bej
OS and Director General (R&M)

सत्यमेव जयते

स्वच्छ भारत
एक कदम स्वच्छता की ओर

भारत सरकार, रक्षा मंत्रालय
अनुसंधान तथा विकास संगठन
101, डी.आर.डी.ओ. भवन
राजाजी मार्ग, नई दिल्ली – 110 011 भारत
Government of India, Ministry of Defence
Defence Research and Development Organisation
101, DRDO Bhawan
Rajaji Marg, New Delhi - 110 011

संदेश

यह अत्यंत प्रसन्नता का विषय है कि **कृत्रिम ज्ञान तथा रोबोटिकी केंद्र (केयर), बेंगलुरु** अपनी हिन्दी गृह पत्रिका **'सुविज्ञ'** के तृतीय तकनीकी अंक का प्रकाशन करने जा रहा है। किसी केंद्र द्वारा राजभाषा हिंदी में किसी पत्रिका का तकनीकी अंक प्रकाशित करना उस केंद्र में राजभाषा के विकास की ओर लिए जा रहे प्रयत्नों को प्रदर्शित करता है। भारत सरकार की राजभाषा नीति एवं आदेशों के अनुपालन की दिशा में यह एक सराहनीय प्रयास है।

'सुविज्ञ' का यह तकनीकी अंक वैज्ञानिकों को उनके कार्यक्षेत्र में प्रयोग हो रही नवीन तकनीक को राजभाषा हिंदी के माध्यम से आम जनमानस तक पहुंचाने में बहुत ही सहायक सिद्ध होगा। **'सुविज्ञ'** के पाठकों को निश्चित ही इस अंक में रोचक जानकारी तथा विज्ञान के क्षेत्र में प्रयुक्त नवीन तकनीक को जानने एवं समझने का मौका मिलेगा।

मुझे आशा है कि **'सुविज्ञ'** के इस तकनीकी अंक के प्रकाशन से केन्द्र में वैज्ञानिक, अधिकारी एवं कार्मिकों की रचनात्मकता में वृद्धि होगी। मैं केन्द्र के निदेशक एवं सभी अधिकारियों एवं कर्मचारियों को शुभकामनाएं देते हुए इस अंक के सफल प्रकाशन की कामना करता हूं।

(पुरुषोत्तम बेज)

डॉ. रविन्द्र सिंह
उत्कृष्ट वैज्ञानिक एवं निदेशक

Dr. Ravindra Singh
OS and Director

सत्यमेव जयते

स्वच्छ भारत
एक कदम स्वच्छता की ओर

भारत सरकार, रक्षा मंत्रालय
रक्षा अनुसंधान तथा विकास संगठन
संसदीय कार्य, राजभाषा तथा संगठन पद्धति निदेशालय
र.अ.वि.सं. मुख्यालय, डी.आर.डी.ओ. भवन
राजाजी मार्ग, नई दिल्ली – 110 011
Government of India, Ministry of Defence
Defence Research and Development Organisation
Directorate of Parliamentary Affairs, Rajbhasha and O&M
DRDO Bhawan, Rajaji Marg, New Delhi - 110 011

संदेश

मुझे यह जानकर अत्यंत हर्ष का अनुभव हो रहा है कि **कृत्रिम ज्ञान तथा रोबोटिकी केंद्र (केयर), बेंगलुरु** अपनी वार्षिक हिन्दी गृह पत्रिका **'सुविज्ञ'** के तृतीय तकनीकी अंक का प्रकाशन करने जा रहा है। राजभाषा हिंदी राष्ट्रीय एकता, संस्कृति और संपर्क का सबसे उत्तम सूत्र है। इस प्रकार के प्रयासों से संघ की राजभाषा नीति के कार्यान्वयन को एक नई दिशा मिलेगी।

राजभाषा नीति का कार्यान्वयन केवल हमारे लिए संवैधानिक दायित्व ही नहीं, अपितु सांस्कृतिक एकता का भी प्रतीक है। मेरा ऐसा मानना है कि केंद्र के दैनिक सरकारी कार्यों के साथ-साथ तकनीकी कार्यों में भी इसकी उपयोगिता बढ़ाने की आवश्यकता है। **'सुविज्ञ'** का यह तकनीकी अंक निश्चित ही इस उद्देश्य की पूर्ति में सहायक साबित होगा।

इस अवसर पर मैं केन्द्र के निदेशक सहित **'सुविज्ञ'** के तकनीकी अंक से जुड़े सभी लेखकों एवं पत्रिका प्रकाशन से संबंधित सभी अधिकारियों/कर्मचारियों को शुभकामनाएं देता हूं।

(डॉ. रविन्द्र सिंह)

डॉ. ऋतुराज कुमार
उत्कृष्ट वैज्ञानिक एवं निदेशक

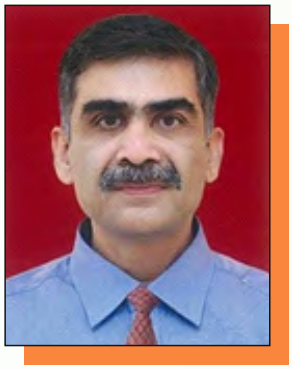
Dr. Rituraj Kumar
OS and Director

सत्यमेव जयते

स्वच्छ भारत
एक कदम स्वच्छता की ओर

कृत्रिम ज्ञान तथा रोबोटिकी केंद्र
रक्षा अनुसंधान तथा विकास संगठन
रक्षा मंत्रालय, भारत सरकार
सी.वी. रमन नगर, बेंगलुरु – 560 093, भारत
Centre for Artificial Intelligence & Robotics
Defence Research & Development Organization
Ministry of Defence, Government of India
C.V. Raman Nagar, Bengaluru – 560 093, India

संदेश



अत्यंत प्रसन्नता का विषय है कि **कृत्रिम ज्ञान तथा रोबोटिकी केंद्र (केयर),** बेंगलूरु अपनी वार्षिक हिन्दी पत्रिका **'सुविज्ञ'** तकनीकी अंक-3 का प्रकाशन करने जा रहा है। इस पत्रिका का उद्देश्य केवल राजभाषा नीति के अनुपालन तक सीमित न होकर सरल और सहज हिन्दी में केन्द्र के वैज्ञानिक एवं तकनीकी अनुसंधान कार्य को सामान्य रूप से जनमानस तक पहुंचाना भी है।

मैं पत्रिका के सफल प्रकाशन के लिए केन्द्र के सभी अधिकारियों एवं कर्मचारियों को हार्दिक बधाई देता हूँ तथा आशा करता हूं कि भविष्य में भी इस प्रकार के सफल एवं ज्ञानवर्धक अंक नियमित रूप से प्रकाशित होते रहेंगे।

शुभकामनाओं सहित।

(डॉ. ऋतुराज कुमार)

टी. आर. उषा कुमारी
वैज्ञानिक 'एफ' एवं
उपाध्यक्षा, रा.भा.का.स.

T.R. Usha Kumari
Scientist 'F' &
Vice-chairperson, OLIC

सत्यमेव जयते

स्वच्छ भारत
एक कदम स्वच्छता की ओर

कृत्रिम ज्ञान तथा रोबोटिकी केन्द्र
भारत सरकार, रक्षा मंत्रालय
रक्षा अनुसंधान तथा विकास संगठन
सी.वी. रामन नगर, बेंगलूरू – 560 093, भारत
Centre for Artificial Intelligence & Robotics
Government of India, Ministry of Defence
Defence Research and Development Organisation
C.V. Raman Nagar, Bengaluru - 560 093, India

संपादकीय

कृत्रिम ज्ञान तथा रोबोटिकी केंद्र के हिंदी तकनीकी पत्रिका '**सुविज्ञ**' के तृतीय अंक को आपके समक्ष प्रस्तुत करते हुए मुझे अत्यंत खुशी हो रही है। हमने इस अंक में भी श्रेष्ठतम तकनीकी लेखों को सम्मिलित किया है। मैं इसके लिए संपादक मंडल के सदस्यों के साथ सभी लेखों को अपना आभार व्यक्त करती हूँ।

इस संबंध में आपके बहुमूल्य विचार व सुझाव प्रतीक्षित है ताकि आगामी अंकों को और अधिक उत्कृष्ट बनाया जा सके।

(उषा कुमारी)

सार प्रतिबिंबों पर वस्तु संसूचन

श्रीमती अणिमा मिश्रा शर्मा, वै 'ई'

सारांश:

सिन्थेटिक अपर्चर रेडार (SAR) प्रतिबिम्बों की रव (Noise) से अत्यधिक दूषित होने की प्रवृत्ति होती है,इसके फलस्वरूप वस्तु संसूचन (Object Detection) अथवा लक्ष्य अभिज्ञान (Target Recognition) की प्रक्रिया अत्यंत क्लिष्ट तथा चुनौतीपूर्ण कार्य बन जाती है। मुख्यतः सार व्यापक रूप से समुद्रीय निरीक्षण हेतु एक विकसित सक्रिय सूक्ष्म तरंग संवेदक (Sensor) है। दूरस्थ संवेदन समुदाय (Remote Sensing Community) हेतु समुद्रीय निरीक्षण मिशनों के लिए सार प्रतिबिम्बों में स्वतः नौका का वर्गीकरण तथा संसूचन एक महत्त्वपूर्ण कार्य है। इस शोध पत्र के योगदान निम्नलिखित हैं- सर्वप्रथम, सार्वजनिक स्तर पर उपलब्ध सार डेटासेटों का मूल्यांकन तथा तुलनात्मक मापदंडों की व्याख्या की गई है। द्वितीय, साहित्य में बहु चर्चित तथा आधुनिक डीप तंत्रिका तंत्र पर आधारित वस्तु संसूचन अथवा लक्ष्य अभिज्ञान हेतु प्रणालियों की योग्यता का सार प्रतिबिंबों पर उनकी उपयोगिता प्रदर्शित की गयी है। प्रस्तावित प्रणाली द्वारा प्राप्त विभिन्न डेटासेटो के अंतर्गत जटिल द्रश्य पर प्रोत्साहक प्रयोगात्मक परिणाम प्रस्तुत किए गए हैं । यह शोध पत्र शोधकर्ताओं को इस क्षेत्र विशेष में शोध करने हेतु समर्थ बना सकता है।

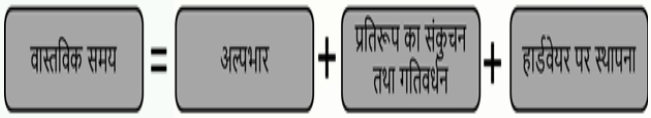
संकेत शब्दावली- कन्वोल्यूशनल तंत्रिका तंत्र, डीप प्रशिक्षण, सार प्रतिबिम्ब, वस्तु संसूचन, नौका संसूचन, संगणक द्रष्टि

भूमिका

सिन्थेटिक अपर्चर रेडार (SAR) सम्पूर्ण दिन तथा सम्पूर्ण मौसम (All-day and All-weather) में उपयोग होने वाला संवेदक है और इस संवेदक का प्रयोग विभिन्न क्षेत्रों में जैसे सैनिक , कृषि सम्बन्धी, भूगर्भीय, पर्यावरणीय, समुद्रीय इत्यादि क्षेत्रों में व्यापक रूप से होता है। सार नौका संसूचन (SAR ship detection) समुद्रीय (Marine Monitoring) निगरानी में अवैध माहिगिरी (Illegal Fishing), तेल गिरावट पहचान (Oil Spill Detection) तथा यातायात व्यवस्था (Maritime Traffic Management) के लिए एक बहुत ही महत्वपूर्ण उपकरण है। पारम्परिक संसूचन की कलनविधियाँ स्थायी अवास्तविक अलार्म दर (Constant False Alarm Rate(CFAR) पर आधारित होती हैं। यह कलनविधियाँ सर्वप्रथम अव्यवस्था (Clutter) को रूप देती (Models) हैं , इसके पश्चात अवास्तविक अलार्म दर (FAR) के अनुसार सीमा रेखा(Threshold) का मूल्य (Value) निश्चित करती हैं। प्रतिबिम्ब में उपस्थित पिक्सलों का मूल्य जब सीमा रेखा के मूल्य से अधिक होता है तो वे नौका पिक्सलों में वर्गीकृत किए जाते है , तथा सीमा रेखा के मूल्य से नीचे वाले पिक्सलों को पृष्ठभूमि में वर्गीकृत किया जाता है। इस कलनविधि की उपलब्धि मुख्यतः समुद्र की अव्यवस्था के सांख्यिकीय प्रतिरूपण (Modeling) तथा चयनित प्रतिरूप के मापदण्डों के आकलन पर निर्भर करती है। सामान्य द्रश्य हेतु पारम्परिक कलनविधियाँ अच्छे परिणाम दर्शाती हैं परन्तु जटिल तट से दूर दृश्यों के लिए अधिकतर अवास्तविक तथा न्यूनतम स्तर के परिणाम प्राप्त होते हैं। अवास्तविक अलार्म दर (CFAR) के पश्चात विभेदन का उपयोग नौका क्षेत्र और नौका विहीन क्षेत्र के वर्गीकरण हेतु किया जाता है। विभेदन हेतु विभिन्न विशेषताओं जैसे लम्बाई,चौड़ाई, हॉग (HOG), एलबीपी(LBP),सर्फ(-SURF) आदि का उपयोग किया जाता है। वर्गीकरण हेतु एसवीएम (SVM), एमएलपी (MLP) आदि कलनविधियों का उपयोग किया जाता है। 2012 में डीप प्रशिक्षण पर आधारित कलनविधियों के प्रचलित होने के पश्चात, कलनविधियों के परिणामों की शुद्धता में अत्यधिक वृद्धि हुई है। डीप प्रशिक्षण पर आधारित कलनविधियाँ आद्योपान्त (End-to-end) रूप से कार्य करती हैं। ये कलनविधियाँ विभिन्न प्रकार के जटिल दृश्यों के लिए अच्छी गुणवत्ता के साथ स्वयं को रूपान्तरित कर लेती हैं। इन कलनविधियों के लाभदायक होने के कारण, सार के शोधकर्ताओं ने इन कलनविधियों का उपयोग करना आरंभ कर दिया है।

डीप प्रशिक्षण पर आधारित संसूचक मुख्यतः कन्वोल्यूशनल तंत्रिका तंत्र (सी.एन.एन.(CNN)) द्वारा विशेषताओं से निष्कर्ष निकालने की क्षमता पर आधारित होते हैं। अच्छी उपलब्धि प्राप्त करने हेतु, अधिकतर सी.एन.एन. गहरे और विस्तीर्ण होते हैं, और इनकी अभिकलनात्मक जटिलता तथा मेमोरी का व्यय

बहुत अधिक होता है। उदाहरण के लिए एलेक्सनेट(-AlexNet) हेतु 60 मिलियन मापदण्डों के गणन की आक्श्यकता होती है जहाँ पर इस नेट में पांच कन्वोल्यूशनल पटल और तीन पूर्ण (Fully Connected Layers) रूप से जुड़े हुए पटलों की आवश्यकता होती है। इतने बड़े प्रतिरूप (Model) को सीमा पर उपलब्ध संकीर्ण संगणन तथा मेमोरी वाले उपकरणों पर कार्यरत करना बहुत ही कठिन होता है। वास्तविक समय में सार नौका संसूचन चलाने हेतु, हल्के तन्त्र के परिकल्पना , प्रतिरूप के संकुचन, गति वर्द्धन तथा हार्डवेयर पर प्रतिरूप स्थापित करने की आवश्यकता होती है। चित्र 1 इस प्रक्रिया का विवरण देता है।



चित्र 1

सार प्रतिबिंबों में वस्तु संसूचन की प्रक्रिया से सम्बंधित कई जटिल चुनौतियाँ पायी जाती हैं जैसे कि जटिल पृष्ठभूमि के कारण व्यवधान (Complex Background Interference),वस्तुओं के अनियंत्रित अभिविन्यास (Arbitrary Orientation), वस्तु अथवा नौका विशेष की विशिष्टताओं में विविधता (Feature Variations), अत्यधिक असमान वस्तुओं का घनत्व (Non-Uniform Object Densities), विस्तृत दृष्टिकोण अनुपात (Large Aspect Ratio) तथा सूक्ष्म आकार की नौकाओं से सम्बंधित विशिष्टता इत्यादि ।

निम्नलिखित अनुभागों में अत्यधिक प्रचलित सार्वजनिक डेटासेटों का संक्षिप्त में वर्णन किया गया है तथा डीप प्रशिक्षण पर आधारित विभिन्न कलनविधियों का उनकी गति तथा शुद्धता के आधार पर तुलनात्मक विवरण दिया गया है। इसके पश्चात हम विभिन्न अत्याधुनिक प्रशिक्षण प्रणालियों पर विचार विमर्श करेंगे तथा कुछ परिणाम भी प्रस्तुत करेंगे।

साहित्य में उपस्थित डेटासेट

डेटा चालित (Driven) संगणक दृष्टि अनुसंधान हेतु पूर्णरूप से व्याख्यातित डेटासेटों (Well-Annotated Datasets) का बहुत ही महत्वपूर्ण स्थान है। इस अनुभाग में, वस्तु संसूचन हेतु सार प्रतिबिंबों युक्त डेटासेटों का निरीक्षण करेंगे।

सार्वजनिक डेटासेटों का विवरण

चित्र 2 नौका संसूचन हेतु सार्वजनिक डेटासेटों के विषय में संक्षिप्त जानकारी प्रदर्शित करता है।

चित्र 2

एसएसडीडी (SSDD) सार प्रतिबिम्बों में नौका संसूचन हेतु सबसे पहला डेटासेट है। इस डेटासेट द्वारा सार नौका संसूचन की तकनीक ने डीप प्रशिक्षण के युग में पहला कदम रखा है। इसके पश्चात, शोधकर्ताओं ने सार प्रतिबिम्बों में नौकाओं के संसूचन हेतु विभिन्न कलनविधियों को प्रस्तावित किया। डीप प्रशिक्षण पर आधारित कलनविधियों को कार्यरत होने के लिए, प्रचुर मात्रा में डेटा की आवश्यकता होती है, विशाल प्रतिरूप के प्रशिक्षण हेतु अत्यधिक प्रतिबिम्बों की आवश्यकता होती है। एसएसडीडी (SSDD) डेटासेट में अपर्याप्त मात्रा में डेटा की समस्या है। चित्र 2 इस डेटासेट के कुछ नमूने प्रतिबिम्ब प्रस्ततु किए गए हैं।

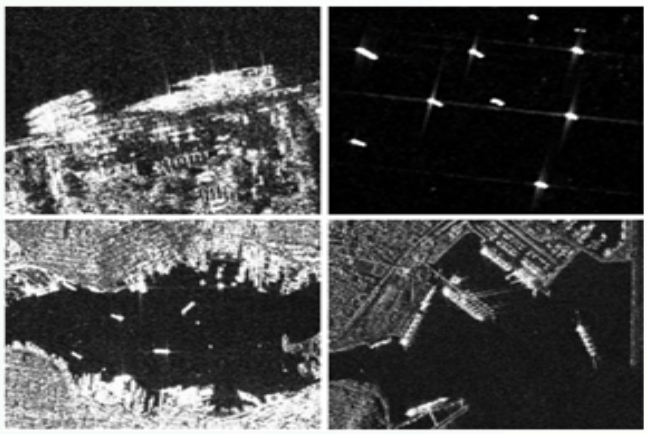
डेटासेट	श्रोत	विभेदन क्षमता	प्रतिविम्ब का आकार	प्रतिविम्ब/नौकाओं की संख्या	एनोटेशन
एसएसडीडी (एसएसडीडी+)	रेडारसेट-2 टेरासार सेंटीनेल-1	1m-15m	190-668	1160-2456	वर्टिकल ओरिएंटेड
सार-शिप-डेटासेट	गाओफेन-3 सेंटीनेल-1	3m-25m	256 x 256	43918/595 35	वर्टिकल
एयर-सारशिप-1.0 एयर-सारशिप-2.0	गाओफेन-3	1m, 3m	3000 x 3000 1000 x 1000	31 300	वर्टिकल
एचआरएसआईडी	सेंटीनेल-1 टेरासार	0.5m, 1m, 3m	800 x 800	5604/116 951	पोलिगोन
एलएस-एसएसडीडी-वी1.0	सेंटीनेल-1	5m, 20m	24000 x 16000	15/6015	वर्टिकल
ओफीसियल-एसएसडीडी एसआरएसडीडी-v1.0	गाओफेन-3 गाओफेन-3	1m	1024 x 1024	666 x 2275	पोलिगोन ओरिएंटेड
आरएसडीडी-सार	टेरासार	2m 20m	512 x 512	7000/10 263	ओरिएंटेड

तालिका - 1

तालिका-1 से हम देख सकते हैं की अधिकतर डेटासेट वर्टिकल बॉन्डिंग बॉक्स से एनोटेट किए गए हैं। एसएसडीडी+, एस.आर.एस.डी.डी.-v1.0, तथा आर.एस.डी.डी.-सार ओरिएंटेड बॉन्डिंग बॉक्स से लेबल किए गए हैं। वहीं एच.आर.एस.आई.डी तथा ऑफिसियल-एसएसडीडी पॉलिगन बॉन्डिंग बॉक्स द्वारालेबल किए गए हैं।

एसएसडीडी (SSDD), एसएसडीडी+ (SSDD+) तथा ऑफिसियल-एसएसडीडी (Official-SSDD):

एसएसडीडी 2017 बिग सार डेटा (2017BIGSAR-DATA) के एक सम्मेलन में प्रस्तावित किया गया था। इस डेटासेट में 1160 प्रतिबिम्बों तथा 2456 नौकायें विद्यमान हैं। डेटा के स्रोत रेडारसेट-2, टेरासार, तथा सेंटीनेल-1 द्वारा 1m से 15m विभेदन क्षमता पर संगृहीत किए गए हैं। लम्बाई अथवा चौड़ाई 600 पिक्सलों के आस-पास है। एसएसडीडी+, एसएसडीडी का संशोधित रूप है। निष्पक्ष प्रयोगात्मक तुलना हेतु ऑफिसियल-एसएसडीडी को प्रस्तावित किया गया। यह बॉन्डिंग बॉक्स, घूर्णन युक्त बॉन्डिंग बॉक्स तथा पॉलिगन विभाजन का समावेश करता है।

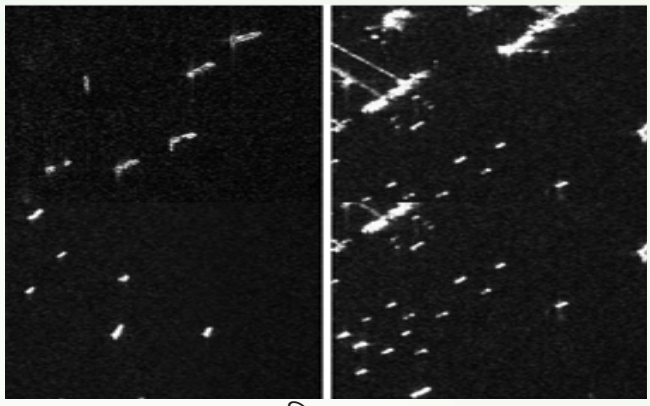


चित्र 3

चित्र 3, एसएसडीडी (SSDD), एसएसडीडी+ (SSDD+) तथा ऑफिसियल-एसएसडीडी (Official-SSDD) के कुछ नमूने दर्शाता है।

सार-शिप डेटासेट:

एसएसडीडी सार-शिप डेटासेट सार्वजनिक रूप से मार्च 29, 2019 को प्रदर्शित हुआ। इस डेटासेट के स्रोत 102 चाईनीज गाओफेन-3 (Gaofen-3) तथा 108 सेंटीनेल-1 है। इसमें 256 x 256 पिक्सलों के आकार की 43,819 चिप्स हैं, और 59,535 विविध स्केल की नौकाएं विद्यमान हैं। इन प्रतिबिम्बों की विभेदन क्षमता 3m से

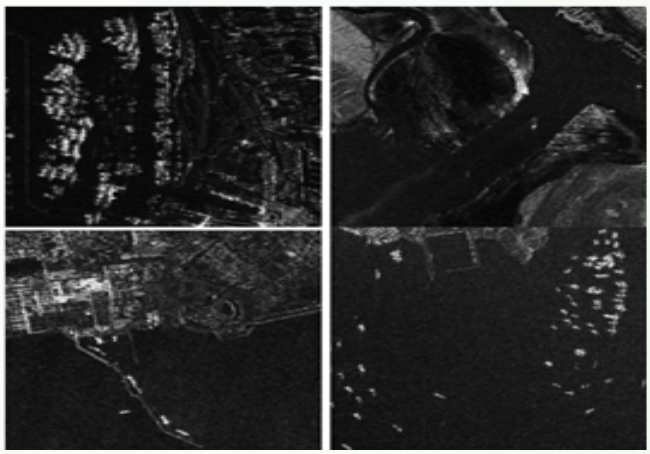


चित्र 4

25m है। नौकाएं बहुत छोटे आकार की हैं और पृष्ठभूमि अत्यधिक जटिल है। चित्र 4 में सार-शिप डेटासेट के कुछ नमूने प्रतिबिम्ब दिखाए गए हैं।

एयर-सारशिप डेटासेट:

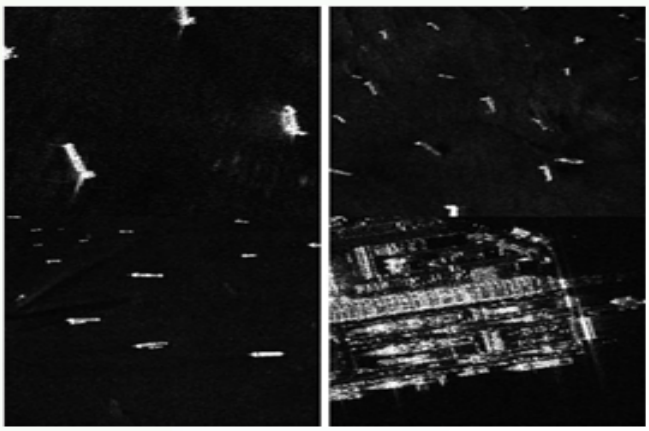
एयर-सारशिप-1.0 दिसंबर 1, 2019 में प्रस्तावित किया गया है। इस डेटासेट में उच्च विभेदन क्षमता युक्त विशालकाय-स्केल के प्रतिबिम्ब हैं। गाओफेन-3 से अभिग्रहित 31 प्रतिबिम्ब हैं। इसमें बंदरगाह (Harbors), टापू (Islands), चट्टान (Reefs) तथा समुद्रीय सतह (Sea Surface) जैसी वस्तुओं के वर्ग उपस्थित हैं। प्रशिक्षण के लिए 21 प्रतिबिम्ब तथा परीक्षण के लिए 10 प्रतिबिम्ब हैं। इन प्रतिबिम्बों की विभेदन क्षमता 1m तथा 3m है। प्रतिबिम्बों का आकार 3000 x 3000 पिक्सल है। एयर-सारशिप-2.0, 25 अगस्त 2021 में प्रस्तावित हुआ है। गाओफेन-3 से लिए हुए 300 प्रतिबिम्ब हैं। प्रतिबिम्बों का आकार 1000 x 1000 पिक्सल है। चित्र 5 में इस डेटासेट के कुछ प्रतिबिम्ब दर्शाये गए हैं।



चित्र 5

एच.आर.एस.आई.डी:

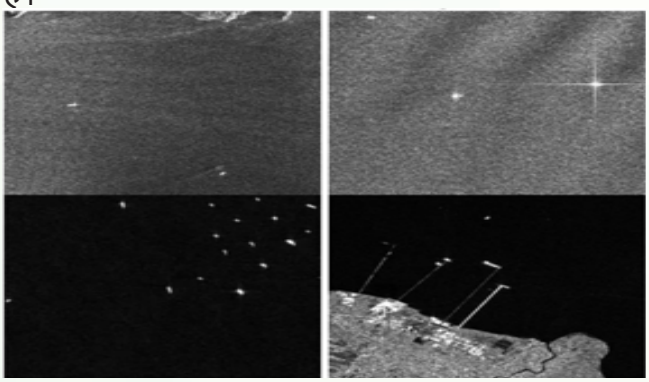
एच.आर.एस.आई.डी डेटासेट 29 जून, 2020 को प्रस्तावित हुआ है। एच.आर.एस.आई.डी डेटासेट में 99 सेंटीनेल-1B प्रतिबिम्बों , 36 टेरासार-एक्स प्रतिबिम्बों ,तथा 1 टेनडम्-एक्स प्रतिबिम्ब का समावेश है। इनकी विभेदन क्षमता क्रमशः 0.5m , 1m , तथा 3m है। इनका एनोटेशन पॉलिगन से किया गया है। इनके प्रतिबिम्बों का माप 800 x 800 पिक्सल है। चित्र 6 में इस डेटा के कुछ प्रतिबिम्बों को दर्शाया गया है।



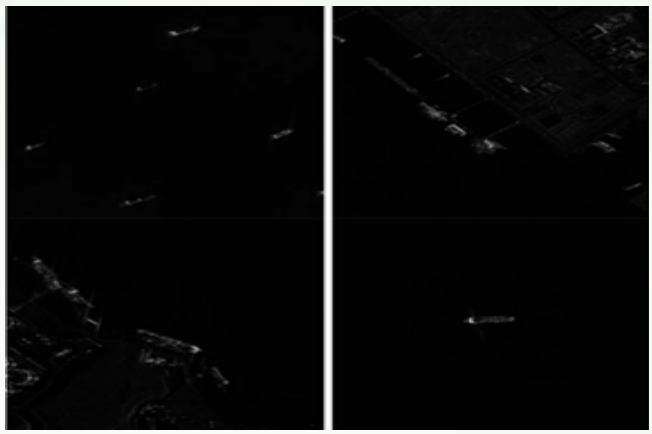
चित्र 6

एल.एस.-एस.एस.डी.डी.-v1.0:

यह डेटासेट 15 सितम्बर, 2020 को प्रस्तावित किया गया है। इस डेटा का स्रोत सेंटीनेल-1 है तथा इस डेटा की विभेदन क्षमता 5m तथा 20m है। इस डेटासेट में 15 विशालकाय सार प्रतिबिम्ब हैं जिनको विशेषज्ञों, स्वतः अभिज्ञान प्रणाली तथा गूगल अर्थ द्वारा लेबल किया गया है। इस डेटासेट में प्रत्येक प्रतिबिम्ब को 800 X 800 पिक्सलों के 600 उप-प्रतिबिम्बों में विभाजित किया गया है। इस डेटासेट में 6015 नौकाओं का समावेश है। चित्र 7, में इस डेटासेट के कुछ प्रतिबिम्बों को दर्शाया गया है।



चित्र 7

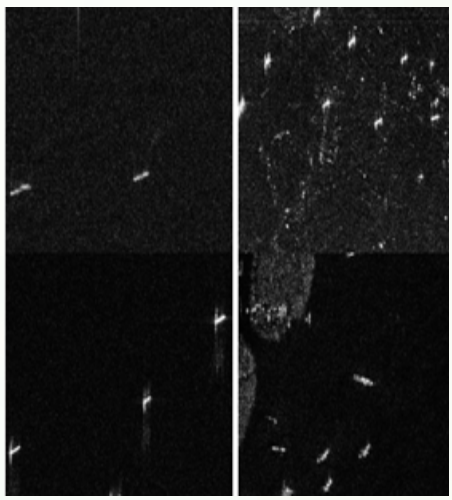


चित्र 8

एस.आर.एस.डी.डी.-v1.0:

यह डेटासेट 15 दिसम्बर 2021 को प्रस्तावित किया गया। इस डेटासेट को 1m विभेदन क्षमता पर गाओफेन-3 स्रोत द्वारा अभिग्रहित किया गया है। एनोटेशन, ओरीएंटेड बॉन्डिंग बॉक्स द्वारा किया गया है। इस डेटासेट में 666 प्रतिबिम्बों का समावेश है तथा छह प्रकार के वर्गों की नौकाएं सम्मलित हैं: अयस्क–तेल नौकाएं (166), विशाल कार्गो नौकाएं(2053), मत्स्य-ग्रहण नौकाएं (288), कानून प्रवर्तन नौकाएं (25), ड्रेजर नौकाएं (263), कंटेनर नौकाएं (89)। इस डेटासेट में प्रतिबिम्बों का आकार 1024 x 1024 है। चित्र 8, में इस डेटासेट के कुछ नमूने प्रस्तुत किए गए हैं।

(चित्र 9) --->



आर.एस.डी.डी.-सार:

यह डेटासेट 7 जुलाई, 2021 में प्रस्तावित किया गया। डेटा के स्रोत गाओफेन-3 और टेरासार हैं तथा जिनकी विभेदन क्षमता 2m से 20m है। इस डेटासेट में 84 जीएफ3 द्रश्य, तथा 41 टेरासार-एक्स विशालकाय द्रश्य हैं। चित्र 9, इस डेटासेट के कुछ नमूने प्रस्तुत करता है।

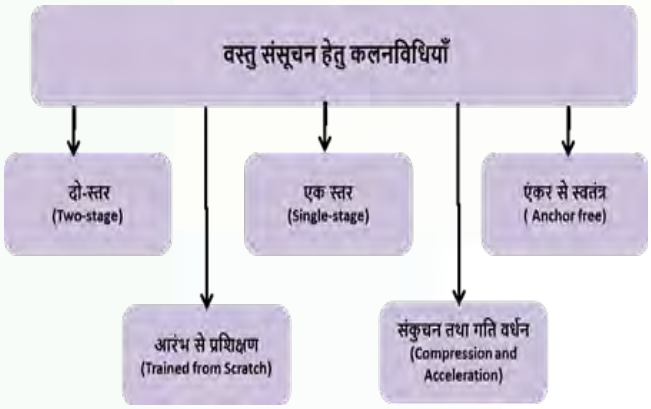
आवश्यक हार्डवेयर:

वस्तु संसूचन हेतु सी.एन.एन.(CNN) पर आधारित

कलनविधियों को कार्यरत होने के लिए एक समर्पित जीपीयू कार्ड की आवश्यकता होती है, यह कलनविधियाँ जीपीयू के विभिन्न कोरों का उपयोग भलीभांति करती हैं।

कलनविधियाँ (METHODS):

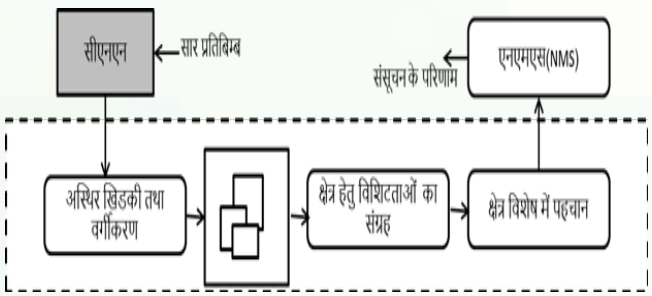
वस्तु संसूचन हेतु साहित्य में विभिन्न प्रकार की कलनविधियाँ प्रस्तावित की गई हैं। विभिन्न स्तरों के अनुसार, डीप-प्रशिक्षण पर आधारित वस्तु संसूचन की कलनविधयों को एक स्तर तथा दो-स्तर संसूचकों में विभाजित किया गया है। इस क्षेत्र में प्रगति के साथ दोनों ही प्रकार की कलनविधियों ने गति तथा शुद्धता में वृद्धि प्राप्त की है। चित्र 10 में वस्तु संसूचन हेतु विभिन्न प्रकार की कलनविधियों का वर्गीकरण किया गया है।



चित्र 10

कुछ और कलनविधियाँ जैसे योलो-v1 (YOLOv1), योलो- v2 (YOLOv2), योलो-v3 (YOLOv3), योलो-v4 (YOLO-v4), योलो-v5 (YOLOv5), तथा योलोएक्स (YOLOX) एक स्तर और एंकर से स्वतंत्र कलनविधियाँ हैं।

दो स्तर पर आधारित संसूचक

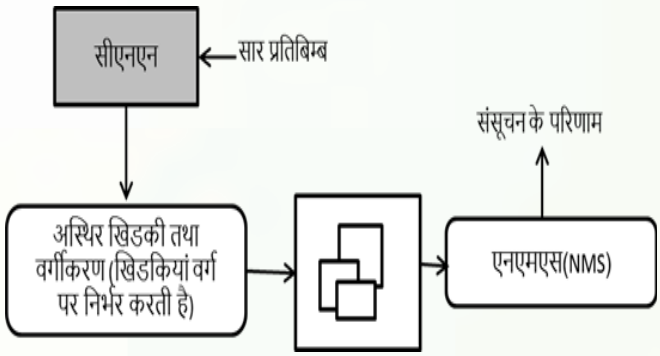


चित्र 11

चित्र 11, दो स्तर पर आधारित वस्तु संसूचन की कलनविधि की पाइपलाइन को दर्शाता है। यह सी.एन.एन. वस्तुओं के वर्गीकरण तथा संसिचन की प्रक्रिया में एंकर बॉक्स की गणना दो स्तर पेपर करते हैं। पारम्परिक दो स्तर पर आधारित संसूचक कुछ इस प्रकार हैं- आर-सी.एन.एन. (R-CNN), एस.पी.पी.-नेट (SPP-Net), फास्टर आर-सी.एन.एन. (Faster R-CNN) से आर-एफ.सी.एन. (R-FCN) इत्यादि । फास्टर आर-सी.एन.एन.(Faster R-CNN) दो स्तर संसूचन की एक आधार कलनविधि है।

एक-स्तर पर आधारित संसूचक

चित्र 12, एक-स्तर पर आधारित कलनविधियों की सम्पूर्ण व्यवथा को दर्शाता है। यहाँ पर कन्वोल्यूशन तंत्र द्वारा एक साथ ही वस्तुओं का वर्गीकरण तथा बॉन्डिंग बॉक्स की गणना की जाती है। ये संसूचक प्रतिबिम्ब को एक बार देख कर ही, वस्तुओं की जानकारी प्राप्त करते है कि वस्तु क्या है और प्रतिबिम्ब में वह कहाँ पर स्थित है। ये संसूचक मानवीय नेत्र के सामान हैं। ये संसूचक दो स्तर वाले संसूचकों कि तुलना में अत्यधिक तीव्र हैं। योलो(Y-OLO), एसएसडी(SSD), रेटीनानेट(RetinaNet), तथा कॉर्नरनेट(CornerNet) इत्यादि कुछ प्रचलित एक-स्तर पर आधारित कलनविधियाँ हैं। इन सारे एक-स्तर कलनविधियों में, योलो सर्वाधिक लोकप्रिय कलनविधि है। यह कलनविधि परिणामों की गति तथा शुद्धता में एक अच्छा सामंजस्य स्थापित करती है।



चित्र 12

एंकर से स्वतंत्र संसूचक

डीप प्रशिक्षण पर आधारित वस्तु संसूचन की कलनविधियों का मुख्यतः वर्गीकरण दो प्रकार से किया गया है- एंकर पर आधारित तथ एंकर मुक्त विधियाँ। एंकर बॉक्स की आवश्यकता वस्तु को प्रतिबिम्ब के भीतर एक क्षेत्र विशेष में ढूँढने के लिए होती है। एंकर-मुक्त संसूचक एक नवीन धारणा स्थापित करता है जिसमें कि पूर्व-परिभाषित एंकर बॉक्स कि आवश्यकता नहीं होती

है। यह कलनविधि विशिष्ट मैप द्वारा बहुत सारे लक्ष्य के बिंदुओं का पूर्वानुमान लगाता है। इस कलनविधि के उदाहरण कुछ इस प्रकार हैं जैसे कॉर्नरनेट, एफकॉस तथा फ़ोवियाबॉक्स इत्यादि।

आरम्भ से प्रशिक्षण

आरम्भ से प्रशिक्षित किए गए प्रतिरूपों द्वारा न केवल उत्कृष्ट शुद्धता प्राप्त होती है अपितु यहाँ पर प्रतिरूप के आकार तथा गणना की मात्रा भी अत्यधिक संक्षिप्त हो जाती है। इन लाभों को देखकर, सार वस्तु संसूचन हेतु इन कलनविधियों का उपयोग किया जाता है।

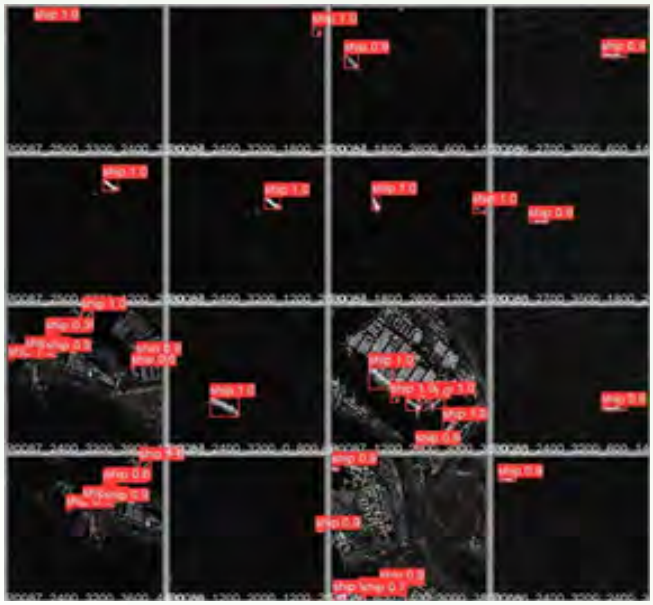
संकुचन तथा गति वर्द्धन

वस्तु संसूचन की कलनविधियों को किसी प्लेटफार्म पर कार्य करवाने हेतु सीमित गणक तथा सीमित मेमोरी के संसाधनों की आवश्यकता होती है। शोधकर्ताओं ने सी.एन.एन. का उपयोग संकुचन तथा गति वर्द्धन हेतु भी किया है। उदाहरण के लिए टेन्सर-आरटी (Tensor-RT), ओ.एन.एन.एक्स. रनटाइम (ONNX RunTime), एन.सी.एन.एन. (NCNN), तथा ओपनविनो (OpenVI-NO)।

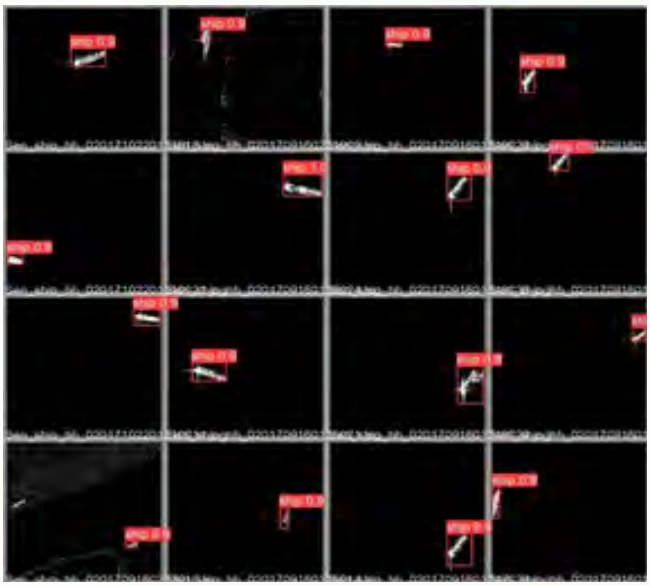
प्रशिक्षण कार्य-प्रणाली तथा परिणाम

किसी नए डेटासेट पर कलनविधि विशेष के प्रतिरूप को प्रशिक्षित करने हेतु सर्वप्रथम डेटा को तैयार करने की आवश्यकता होती है। मुख्यतः डेटासेट का विभाजन तीन भागों में किया जाता है- प्रशिक्षण, प्रमाणीकरण तथा परीक्षण। 60%-70% डेटा का उपयोग प्रतिरूप के प्रशिक्षण हेतु किया जाता है। 20%-25% डेटा को प्रमाणीकरण (Validation) हेतु नियुक्त किया जाता है तथा शेष 15%-20% डेटा का उपयोग परीक्षण हेतु किया जाता है। सामान्यतः प्रशिक्षण की प्रक्रिया 300 इपोक तक इमेजनेट डेटासेट के पूर्वप्रशिक्षित प्रतिरूपों का उपयोग कर क्रियान्वित होती है। प्रतिरूप को सक्षम बनाने हेतु डेटा के वृद्धिकरण के लिए नयी कलनविधियों को प्रस्तावित किया गया है।

यहाँ पर योलो-v5 कलनविधि का उपयोग एच.आर.एस.आई.डी तथा सार-शिप डेटासेट पर प्रतिरूपों का प्रशिक्षण किया गया है। चित्र 13 में एच.आर.एस.आई.डी डेटासेट के कुछ नमूने प्रतिबिम्ब पर संसूचन के परिणाम दर्शाये गए हैं। 300 इपोक पर 94.6% की परिशुद्धता प्राप्त हुई है।



चित्र 13: एच.आर.एस.आई.डी डेटासेट के प्रतिबिम्बों पर परिणाम



चित्र 14: सार-शिप डेटासेट के प्रतिबिम्बों पर परिणाम

चित्र 14 में सार-शिप डेटासेट के कुछ नमूने प्रतिबिम्बों पर वस्तु संसूचन के परिणाम प्रस्तुत किए गए हैं। प्रशिक्षित प्रतिरूप द्वारा 98.5% की परिशुद्धता प्राप्त की गई है।

निष्कर्ष

यह शोध पत्र सार प्रतिबिम्बों में वस्तु संसूचन के बारे में विस्तृत विवरण देता है। यहाँ पर साहित्य में प्रचलित विभिन्न डेटासेटों की समीक्षा की गई है। यह शोध पत्र सार प्रतिबिम्बों में वस्तु संसूचन की प्रक्रिया से सम्बंधित विभिन्न जटिल चुनौतियों पर प्रकाश डालता है। डीप-

प्रशिक्षण पर आधारित सार प्रतिबिम्बों में वस्तु संसूचन हेतु एक-स्तर पर आधारित, दो-स्तर पर आधारित, एंकर से स्वतंत्र, आरम्भ से स्वतंत्र और संकुचन तथा गति वर्द्धन इत्यादि कलनविधियों के बारे में विस्तारपूर्वक जानकारी दी गई है। इन कलनविधियों के अनुप्रयोग हेतु अत्यधिक सशक्त संगणक हार्डवेयर तथा डेटा को लेबल करने की आवश्यकता होती है। डीप फ्रेमवर्क (Deep Framework) का उपयोग कुशलतापूर्वक करने से सार प्रतिबिंबों पर सुचारू रूप से वस्तुओं का संसूचन करना संभव हुआ है।

संदर्भ-

[1] अणिमा मिश्रा शर्मा, "रोबोट के द्वारा एकीकृत वास्तविक समय पर वस्तु का संसूचन", उत्कर्ष 2017.

[2] अणिमा मिश्रा शर्मा, "स्वतंत्र आंतरिक रोबोटिक प्रणाली हेतु द्रश्यात्मक वस्तु का संसूचन", उत्कर्ष 2018.

[3] अणिमा मिश्रा शर्मा, "वस्तु संसूचन पर आधारित विडियो का संक्षिप्तीकरण", उत्कर्ष 2019.

[4] अणिमा मिश्रा शर्मा, "वस्तु संसूचन द्वारा निर्देशित स्वायत्त वाहन हेतु स्वचालित होर्न", उत्कर्ष 2020

[5] अणिमा मिश्रा शर्मा, "सुरक्षा एवं रक्षा अनुप्रयोगों हेतु द्रष्टि अभिज्ञान", उत्कर्ष 2021

[6] अणिमा मिश्रा शर्मा, " आकाशीय एवं उपग्रह प्रतिबिंबों पर वस्तु संसूचन", उत्कर्ष 2022

[7] Jianwei Li, Jie Chen, Pu Cheng, Zhentao Yu Lu Yu and Cheng Chi, " A Survey on Deep-Learning-Based Real-Time SAR Ship Detection", IEEE JOURNAL ON SELECTED TOPICS IN APPLIED EARTH OBSERVATIONS AND REMOTE SENSING, VOL. 16, 2023.

पोस्ट-क्वांटम युग के लिए एक नया बहुपद आधारित ब्लॉक सिफर

डॉ. भूपेंद्र सिंह, वैज्ञानिक-एफ

सारांश

ब्लॉक सिफर मुख्य रूप से संवेदनशील जानकारी की सुरक्षा के लिए एक व्यापक एन्क्रिप्शन तकनीक सुनिश्चित करने के लिए डिज़ाइन किए गए हैं। इन वर्तमान क्रिप्टोग्राफिक तकनीकों को शास्त्रीय और क्वांटम विरोधियों से हमलों की एक श्रृंखला का सामना करने की आवश्यकता होती है। क्रिप्टएनालिसिस तकनीकों में प्रगति और कंप्यूटिंग शक्ति में वृद्धि सिफर को अवरुद्ध करने के लिए लगातार खतरे डालती है। क्वांटम-प्रतिरोधी ब्लॉक सिफर डिजाइन करने के लिए एक उभरती हुई प्रवृत्ति है जो क्वांटम हमलों के खिलाफ लचीला है। वर्तमान और भविष्य के हमलों को कम करने के लिए स्केलेबल, गतिशील और आधुनिक ब्लॉक सिफर विकसित करने के लिए एक बड़ा शोध स्थान और गुंजाइश है। यह पेपर एक नया दृष्टिकोण प्रस्तुत करता है जो बहुपद को क्रिप्टोग्राफिक कुंजी के रूप में उपयोग करता है और कुंजी पीढ़ी, एन्क्रिप्शन और डिक्रिप्शन जैसे अभिनव एल्गोरिदम का एक सेट पेश करता है। ये गतिशील बहुपद शास्त्रीय और क्वांटम सहित विभिन्न प्रकार के हमलों के खिलाफ मजबूती के साथ प्रस्तावित क्रिप्टोग्राफिक एल्गोरिथ्म में प्रवेश करते हैं। बहुपद की गतिशील प्रकृति प्रस्तावित क्रिप्टोग्राफिक एल्गोरिथ्म की सुरक्षा और लचीलापन को बढ़ाती है।

मुख्य शब्द: सममित सिफर, असममित सिफर, एनआईएसटी पीक्यूसी, ब्लॉक सिफर, कुंजी पीढ़ी, एन्क्रिप्शन एल्गोरिदम, डिक्रिप्शन एल्गोरिदम।

परिचय

डेटा गोपनीयता संरक्षण डिजिटल संचार पर सूक्ष्म डेटा की सुरक्षा का एक अनिवार्य हिस्सा है। कम संरक्षित वायरलेस चैनलों पर डेटा हस्तांतरण की उच्च दर के कारण सुरक्षा जोखिम बढ़ रहे हैं। बैंकिंग, वित्तीय, रक्षा और अन्य सभी आवश्यक सेवाओं जैसे सभी आवश्यक सेवाओं पर विभिन्न हमलों का खतरा होता है। डिजिटल ट्रांसमिशन के लिए गोपनीयता, डेटा अखंडता और प्रमाणीकरण (सीआईए) सेवाएं प्रदान करने के लिए पिछले पांच दशकों में क्रिप्टोग्राफिक एल्गोरिदम मौजूद हैं। डिफी हेल्मन [N1] क्रिप्टोग्राफी के क्षेत्र में पहला प्रकाशन है, जिसमें लेखकों ने एक नई सार्वजनिक-कुंजी क्रिप्टोग्राफी पेश की। डीईएस, 3डीईएस, ब्लोफिश, आरसी 6, आईडीईए और एईएस प्रसिद्ध निजी कुंजी क्रिप्टोग्राफी एल्गोरिदम के उदाहरण हैं, जबकि आरएसए, डिफी हेलमैन, ईसीसी और डिजिटल सिग्नेचर सार्वजनिक-कुंजी एन्क्रिप्शन एल्गोरिदम [N2] [N3] के तहत आ रहे हैं। क्वांटम-सुरक्षित एल्गोरिदम समय की आवश्यकता है क्योंकि सभी मौजूदा मानक क्वांटम कंप्यूटर द्वारा उत्पन्न विभिन्न हमलों के प्रति संवेदनशील हैं। शोध का ध्यान शास्त्रीय एन्क्रिप्शन से पोस्ट-क्वांटम क्रिप्टोग्राफी में स्थानांतरित हो रहा है, लोग गतिशील एल्गोरिदम पसंद करते हैं जहां कुंजी ढूंढना बहुत मुश्किल है [N4]।

सममित एन्क्रिप्शन का महत्वपूर्ण पहलू यह है कि एल्गोरिथ्म की शक्ति कुंजी के आकार से निर्धारित होती है और एक हमलावर को सिफर टेक्स्ट से कुंजी या सादे संदेश का अनुमान लगाने की आवश्यकता होगी। क्वांटम कंप्यूटर में क्रिप्टोग्राफिक एल्गोरिदम को तोड़ने की क्षमता होगी। राष्ट्रीय मानक और प्रौद्योगिकी संस्थान (एनआईएसटी) ने एक वैश्विक प्रतियोगिता [N5] भी शुरू की है, जिसमें संगठन ने क्वांटम-सुरक्षित एल्गोरिदम प्रस्तुत करने के लिए आमंत्रित किया है, काइबर फाइनलिस्ट के रूप में खड़ा है और एनआईएसटी द्वारा शुरू की गई पीक्यूसी प्रतियोगिता का एक मजबूत विजेता है। पोस्ट-क्वांटम क्रिप्टोग्राफी के क्षेत्र में, एल्गोरिदम जाली-आधारित, कोड-आधारित, हैश-आधारित और मल्टीवेरिएट-आधारित [N7] पर काम कर रहे हैं। कई चर वाले बहुपद को बहुभिन्नरूपी क्रिप्टोग्राफी में निपटाया जाता है। बहुभिन्नरूपी बहुपद को हल करना एनपी-हार्ड समस्याएं हैं जो इन सुरक्षा एल्गोरिदम की रीढ़ प्रदान करती हैं। बहुभिन्नरूपी बहुपद-आधारित उदाहरणों में तेल और सिरका हस्ताक्षर विधि और रेनबो क्रिप्टोग्राफी एल्गोरिदम [N8] शामिल हैं।

सामान्य तौर पर, बहुपद और उनके प्रक्षेपों को उनके लचीलेपन और गतिशील प्रकृति के कारण क्वांटम

सुरक्षित पाया जाता है। यह पेपर क्वांटम कंप्यूटिंग के खिलाफ सुरक्षा देने के लिए एक नए बहुपद-आधारित ब्लॉक सिफर पर चर्चा करता है। खंड 2 मौजूदा बहुपद-आधारित एन्क्रिप्शन की विस्तृत साहित्य समीक्षा को दर्शाता है, खंड 3 हमारे प्रस्तावित एल्गोरिथ्म की व्याख्या करता है और धारा 4 में पेपर समाप्त होता है और भविष्य का काम दिया गया है।

साहित्य की समीक्षा

प्रेषक से रिसीवर तक डेटा के सुरक्षित संचरण के लिए आज की दुनिया में क्रिप्टोग्राफी आवश्यक है, क्योंकि सभी वार्तालाप, प्रसारण और सूचना का आदान-प्रदान इंटरनेट पर होता है। प्रमाणीकरण, गोपनीयता और अखंडता की गारंटी देने के लिए, डेटा के एन्क्रिप्शन और डिक्रिप्शन के लिए कई क्रिप्टोग्राफिक विधियों को विकसित और कार्यान्वित किया गया है।

यह खंड क्रिप्टोग्राफिक एल्गोरिदम की स्थापना से लेकर हाल की प्रगति तक साहित्य विवरण देता है। क्रिप्टोग्राफी का मूल्यांकन 1976 में डिफी और हेलमैन [N1] द्वारा एक लेख के प्रकाशन के बाद हुआ, क्योंकि कंप्यूटर को दुनिया में पेश किया गया था और दुनिया भर में संचार बहुत आसान हो गया था। हालांकि, संचार संदेश को प्रसारित करने में ईव्सड्रॉपिंग या किसी भी बदलाव के लिए कमजोर हो सकता है। 1976 में, डेटा एन्क्रिप्शन मानक (डीईएस) को राष्ट्रीय मानक ब्यूरो (एनबीएस) द्वारा पेश किया गया था और संघीय सूचना प्रसंस्करण मानकों (एफआईपीएस) द्वारा अनुमोदित किया गया था।

बाद में, वर्ष 1978 में, सार्वजनिक-कुंजी क्रिप्टोग्राफी एल्गोरिथ्म में, रिवेस्ट शमीर और एडलमैन (आरएसए) [N10] ने एक प्रमुख कारक-आधारित एल्गोरिथ्म प्रस्तुत किया जो एक सार्वभौमिक मानक बन गया है, यह पहली तरह का सफलतापूर्वक कार्यान्वित असममित एल्गोरिथ्म है। डिफी और हेल्मन ने 1979 में एक लेख [N11] लिखा जिसमें क्रिप्टोग्राफी और एल्गोरिदम के मौलिक विचारों को शामिल किया गया था जो 1970 के दशक में लोकप्रिय थे। सिमोन [N12] ने 1979 में क्रिप्टोग्राफिक एल्गोरिदम को दो समूहों में विभाजित किया, सममित कुंजी क्रिप्टोग्राफी और असममित कुंजी क्रिप्टोग्राफी। डीईएस को 1981 में अमेरिकन नेशनल स्टैंडर्ड इंस्टीट्यूट (एएनएसआई) द्वारा भी अनुमोदित किया गया था। डीईएस हमलावरों से डेटा को सुरक्षित करने के लिए पर्याप्त शक्तिशाली था, लेकिन इसमें एक दोष है कि कुंजी बिट केवल 56 बिट्स लंबा है, जिसे अब ब्रूट फोर्स हमले से क्रैक किया जा सकता है क्योंकि कंप्यूटर अतीत की तुलना में काफी तेज हैं।

मर्कल और हेलमैन [N14] ने प्रमुख लंबाई की समस्या को हल करने के लिए 1981 में 112 बिट्स सुरक्षा के साथ डीईएस का एक अधिक सुरक्षित ट्रिपल कुंजी संस्करण पेश किया, जिसे 3डीईएस के रूप में जाना जाता है। 1990 में, लाइ और मैसे [N15] ने डेटा एन्क्रिप्शन और ब्लॉक सिफर तकनीकों को अतिरिक्त भ्रम और प्रसार प्रदान करने के लिए एक नया दृष्टिकोण पेश किया। अंतर्राष्ट्रीय डेटा एन्क्रिप्शन एल्गोरिथ्म इस एल्गोरिथ्म (आईडीईए) का नाम है। अन्य सममित कुंजी एल्गोरिदम, जैसे आरसी 4, आरसी 5, और ब्लोफिश [N16], 1990 से 2000 तक डीईएस की तुलना में लंबी कुंजी लंबाई के दिखाई दिए। 2001 में, रिजमेन और डेमेन ने रिजेंडेल एल्गोरिदम विकसित किया, जिसे बाद में नेशनल इंस्टीट्यूट ऑफ स्टैंडर्ड एंड टेक्नोलॉजी (एनआईएसटी) ने एईएस तकनीक [N17] के रूप में अनुमोदित किया। एईएस डीईएस पर कई लाभ प्रदान करता है, जिसमें तेज थ्रूपुट, उन्नयन में आसानी, सॉफ्टवेयर हार्डवेयर, कार्यान्वयन, पोर्टेबिलिटी और लचीलापन शामिल है, इन गुणों के साथ एईएस एक सार्वभौमिक मानक बन गया [N18][N19]।

सममित कुंजियों के उपयोग के बावजूद, सार्वजनिक-कुंजी एन्क्रिप्शन "ट्रैपडोर" कार्यों पर निर्भर करता है, जो गणना करने के लिए सरल हैं लेकिन अतिरिक्त जानकारी के बिना रिवर्स करना मुश्किल है। रिवेस्ट शमीर और एडलमैन (आरएसए) एल्गोरिदम एक लोकप्रिय सार्वजनिक-कुंजी तकनीक है जिसमें कठिन कार्य एक समग्र पूर्णांक [N20] के प्रमुख कारकों की खोज करना है। परिमित क्षेत्रों पर एलिप्टिक वक्र के आधार पर एक नया सार्वजनिक-कुंजी एल्गोरिथ्म कोब्लिट्ज़ एट अल द्वारा सुझाया गया था। एलिप्टिक कर्व क्रिप्टोग्राफी (ईसीसी) के पीछे का सिद्धांत असतत लघुगणक और फैक्टरिंग समस्याओं [N20] पर आधारित है। शोर [N22] ने 1994 में एक एल्गोरिथ्म प्रकाशित किया जिसे बहुपद समय में असतत लघुगणक और कारकीकरण समस्याओं को हल करने के लिए क्वांटम कंप्यूटर पर चलाया जा सकता है। शोर के एल्गोरिदम और क्वांटम कंप्यूटर की उपलब्धता के रहस्योद्घाटन के बाद, आरएसए और ईसीसी जैसे सार्वजनिक-कुंजी

क्रिप्टोग्राफी की सुरक्षा कमजोर हो जाएगी, जिससे सभी क्रिप्टोसिस्टम के लिए गंभीर खतरा पैदा हो जाएगा। बाद में, 1996 में, ग्रोवर [N23] ने एक एल्गोरिथ्म का प्रस्ताव दिया जहां N संख्या डेटा से एक संख्या खोजने की जटिलता O(√N) क्वांटम कंप्यूटर का उपयोग करके है क्योंकि क्वांटम कंप्यूटर एक साथ कई संख्याओं को संसाधित करने में सक्षम हैं। इस दृष्टिकोण से यह स्पष्ट है कि k लंबाई की एक गुप्त कुंजी पर जटिलता O(√2^k)) के साथ हमला किया जा सकता है। सममित कुंजी एल्गोरिथ्म जैसे कि एईएस या अन्य एल्गोरिदम बड़े-क्वांटम कंप्यूटर उपलब्ध होने पर सुरक्षा प्रदान करने के लिए कमजोर हो सकते हैं।

शोधकर्ताओं ने वर्ष 2000 के आसपास कई क्रिप्टो एल्गोरिदम प्रस्तावित किए जब क्वांटम-सुरक्षित क्रिप्टोसिस्टम की आवश्यकता की घोषणा पहली बार की गई थी। बहुपद को असाध्य माना जाता है क्योंकि उनका पुनर्निर्माण एक कठिन समस्या है, फिर भी उनका उपयोग क्रिप्टोसिस्टम विकसित करने के लिए किया जा सकता है। बहुपद के दायरे में, 1983 में, ब्रांडस्टॉर्म [N24] नामक एक शोधकर्ता ने एक क्रिप्टोसिस्टम पर अपना काम प्रकाशित किया जो आरएसए विधि में बड़ी प्राकृतिक संख्याओं के बजाय परिमित क्षेत्रों पर बहुपद का उपयोग करता था। बड़ी प्राकृतिक संख्याओं को बहुपद के साथ प्रतिस्थापित करके, जिनके गुणांक परिमित क्षेत्रों के अनुरूप हैं, लेखक आरएसए को लागू करने में सफल रहा। 1984 में, लिडल [N25] ने कहा कि डेटा एन्क्रिप्शन और डिक्रिप्शन के लिए बहुपद चुनते समय, अत्यधिक सावधानी बरतनी चाहिए। सबसे पहले, एक परिमित क्षेत्र एफक्यू के तत्वों का क्रमपरिवर्तन; यह f: Fq-> Fq, a-> f(a) को बहुपद f(x) द्वारा प्रेरित किया जाना चाहिए। दूसरा, अधिकृत रिसीवर को डिक्रिप्शन उद्देश्यों के लिए एफ फ़ंक्शन के व्युत्क्रम की आसानी से गणना करने में सक्षम होना चाहिए। ये दो मानदंड बहुपद की संख्या को गंभीर रूप से सीमित करते हैं जिनका उपयोग किया जा सकता है। लोगों ने द्विपद के आधार पर नया क्रिप्टोसिस्टम पर शोध किया है, एक प्रकार का चेबिशेव बहुपद। वर्ष 1999 में, बहुपद के बेखबर मूल्यांकन को नौर और पिंकस [N26] द्वारा दर्शाया गया था। अपने अध्ययन में, बॉब एक बहुपद P जानता है और चाहता है कि ऐलिस इनपुट z दिए गए मान P(z) की गणना करे। बॉब जेड को नहीं जानता है, और ऐलिस पी (पी (एक्स के अलावा) के बारे में कुछ और नहीं सीखता है। लेखकों के अनुसार, यह एक मूल्यवान आदिम है, क्योंकि इसका उपयोग न्यूनतम लागत पर छद्म-यादृच्छिक कार्यों को बदलने के लिए किया जा सकता है। बहुपद-आधारित क्रिप्टोग्राफी के आधार पर आगे के अध्ययन को तालिका 1 में वर्णित किया गया है।

प्रकाशन का वर्ष	रचयिता	मूल	सारांश
2003 [N27]	अगस्त और फिनियाज़ August and Finiasz	क्रिप्टोग्राफिक तकनीकों के सिद्धांत और अनुप्रयोगों पर अंतर्राष्ट्रीय सम्मेलन	1999 में, पहला असाध्य बहुपद पुनर्निर्माण समस्या एल्गोरिथ्म एक कठिन समस्या के रूप में प्रकाशित किया गया था। 2003 में, लेखक ने बहुपद पुनर्निर्माण मुद्दे और रीड-सोलोमन कोड डिकोडिंग समस्या के आधार पर एक नया सार्वजनिक-कुंजी सिफर विधि का सुझाव दिया। उनकी प्रस्तावित तकनीक में सार्वजनिक कुंजी की सुरक्षा बहुपद पुनर्निर्माण कठोरता और रीड-सोलोमन एल्गोरिदम की डिकोडिंग कठिनाई पर आधारित है, एन्क्रिप्शन सुरक्षा प्रदान करती है।

2003 [N28]	अगस्त और फिनियाज़ August and Finiasz	क्रिप्टोलॉजी ईप्रिंट पुरालेख।	कोरोन [N29] ने अपनी रिलीज के तुरंत बाद अगस्त के प्रकाशित क्रिप्टोसिस्टम का क्रिप्टएनालिसिस पूरा कर लिया था। अगस्त एट अल ने अपने एल्गोरिदम को संशोधित किया और एक नया क्रिप्टोसिस्टम बनाया जो उनके क्रिप्टोसिस्टम की सुरक्षा में सुधार के लिए कोरोन के हमले के लिए प्रतिरोधी है। एक सीमित क्षेत्र में, उन्होंने ट्रेस ऑपरेटर को नियोजित किया है। हमलों के खिलाफ सुरक्षा प्रदान करने के लिए, सिस्टम में कई नए पैरामीटर प्रस्तावित किए गए थे।
2004 [N30]	कियायस और युंग Kiayias and Yung	क्रिप्टोलॉजी और सूचना सुरक्षा के सिद्धांत और अनुप्रयोग पर अंतर्राष्ट्रीय सम्मेलन	अगस्त और फिनियाज़ के क्रिप्टोसिस्टम ने बहुपद पुनर्निर्माण समस्या के आधार पर एक लेख जारी किया, लेखक ने अपने सिस्टम का क्रिप्टएनालिसिस किया, इसे तोड़ दिया, और प्रदर्शित किया कि यह असुरक्षित है। सादे संदेश को प्राप्त करने के लिए हमलों के दो रूपों पर सार्वजनिक कुंजी और सिफरटेक्स्ट के ज्ञान के आधार पर चर्चा की जाती है। कोरोन का हमला पहला है, जबकि ऑप्टिमल पैरामीटर सेटिंग (सीएपी+) में सिफरटेक्स्ट-ओनली अटैक प्रॉब्लम दूसरा है।
2006 [N31]	सदखान और रुमा Sadkhan and Ruma	सूचना और संचार प्रौद्योगिकी पर दूसरा अंतर्राष्ट्रीय सम्मेलन	सुरक्षा बढ़ाने के लिए, अगस्त क्रिप्टोसिस्टम के गुणों को अपग्रेड किया गया था। बहुपद पुनर्निर्माण समस्याओं में नियोजित बेरेलकैंप-वेल्श एल्गोरिदम या प्रत्यक्ष दृष्टिकोण की तुलना में, लेखक ने निष्कर्ष निकाला कि लैग्रेंज प्रक्षेप का मूल्यांकन एक उपयोगी विधि है।
2013 [N32]	घोष और साहा Ghosh and Saha	कंप्यूटर विज्ञान और सूचना प्रौद्योगिकी	लेखकों ने नेटवर्क सुरक्षा के लिए बहुपद का उपयोग करके एक नया एन्क्रिप्शन एल्गोरिदम प्रस्तावित किया है। उनके प्रस्तावित काम में, गुप्त कुंजी को एक-तरफ़ा फ़ंक्शन और न्यूटन रैप्सन विधि का उपयोग करके विकसित किया गया है। यह गुप्त कुंजी डिजिटल हस्ताक्षर मानक का उपयोग करके स्थानांतरित की जाती है। स्टेग्नोग्राफ़ी का उपयोग करके सिफरटेक्स्ट को एक तस्वीर के पीछे छिपाया जाता है और फिर रिसीवर को स्थानांतरित किया जाता है।
2016 [N33]	सोनिया और अगरवाल Sonia and Aggerval	कंप्यूटर नेटवर्क और सूचना सुरक्षा के अंतर्राष्ट्रीय जर्नल	लेखक ने डेटा सुरक्षा में सुधार के लिए हैश एल्गोरिदम के आधार पर बहुपद संदेश प्रमाणीकरण का एक नया मॉडल प्रस्तावित किया है। बहुपद का उपयोग सुरक्षित हैशिंग एल्गोरिदम SHA-1 और SHA-256 को लागू करने के लिए किया गया था। संदेश को हैश कोड में बदल दिया जाता है और बाद में उनके प्रस्तावित कार्य में डिग्री 80, 100 या 150 के बहुपद फ़ंक्शन में बदल दिया जाता है। रिसीवर के अंत में एक बहुपद संदेश सत्यापन तंत्र लागू किया जाता है। परिणाम प्रसंस्करण लाभ, वितरण अनुपात, ऊर्जा खपत और शुल्क चक्र के संदर्भ में विस्तारित किया गया है।

2017 [N34]	अल-सियाक AL-Siaq	ग्लोबल जर्नल ऑफ प्योर एंड एप्लाइड मैथमेटिक्स	पूर्णांक लंबी लंबाई कुंजी का उपयोग करने के बजाय, लेखक ने एक बहुपद फ़ंक्शन का उपयोग करके एन्क्रिप्शन और डिक्रिप्शन का प्रस्ताव दिया जिसे डिफी हेल्मन कुंजी विनिमय तंत्र का उपयोग करके स्थानांतरित किया जाता है। सुरक्षा में सुधार करने के लिए, बहुपद फ़ंक्शन संख्यात्मक एल्गोरिदम का उपयोग करके सादे संदेश को एन्क्रिप्ट करता है। बाइसेक्शन, फिक्स्ड-पॉइंट पुनरावृत्ति और न्यूटन राहसन एन्क्रिप्शन के लिए उपयोग किए जाने वाले तीन संख्यात्मक तरीके हैं। लेखक के अनुसार, न्यूटन रैप्सन दृष्टिकोण ने अन्य तरीकों की तुलना में पुनरावृत्तियों की कम संख्या में अनुमानित जड़ उत्पन्न की।
2018 [N35]	चेओन एट अल Cheon et al.	क्रिप्टोलॉजी ईप्रिंट संग्रह	गुप्त कुंजी सेटिंग में संदेश वेक्टर लंबाई एल और डिग्री डी बहुपद कार्यक्षमता के लिए, लेखक ने ओ (एल) सिफरटेक्स्ट के साथ कार्यात्मक एन्क्रिप्शन का एक अभिनव सामान्य निर्माण विकसित किया है। दो एन्क्रिप्शन योजनाएं प्रस्तावित हैं, पहली योजना में एक रैखिक अंकगणितीय सर्किट डिक्रिप्शन विधि शामिल है। दूसरी तकनीक सिफरटेक्स्ट को मॉड्यूल संचालन के माध्यम से एक दूसरे के साथ बातचीत करने की अनुमति देती है। प्रस्तावित योजना एक बड़ी डिग्री का समर्थन नहीं कर सकती है।
2020 [N36]	स्टोयानोव और नेडज़िबोव Stoyan-ov and Nedzhibov	समरूपता	बहुपद फ़ंक्शन की जड़ों का अनुमान लगाने के लिए संख्यात्मक तरीकों का उपयोग करने का तरीका जानने के बाद, लेखक ने न्यूटन रैपसन विधि और रोटेशन अनुवाद समीकरण के आधार पर एक एन्क्रिप्शन एल्गोरिदम प्रस्तुत किया। जड़ की खोज के लिए, न्यूटन दृष्टिकोण का उपयोग पहले किया जाता है, और फिर अंतरिक्ष संकुचन समीकरण का उपयोग करके यादृच्छिकता लागू की जाती है। लेखक के अनुसार, इस एन्क्रिप्शन तकनीक का उपयोग सूचना सुरक्षा के लिए किया जा सकता है।

बहुपद आधारित ब्लॉक सिफरिंग

यह खंड बहुपद और प्रक्षेपों के आधार पर एक पूरी तरह से नए ब्लॉक सिफर की व्याख्या करता है। बहुपद एक सामान्य रूप लेते हैं जैसा कि समीकरण (1) के रूप में दर्शाया गया है।

$f(x)= \sum^{i=n}_{i=0} a_i x^i = \prod_{j=1}^{j=n}(x-R_j)$ ..... (1)

जहां ai बहुपद के गुणांक हैं और n बहुपद की डिग्री है और Rj उस बहुपद के मूल हैं। यादच्छिक बहुपद आम तौर पर उनकी गतिशील लंबाई के कारण अप्राप्य नहीं हो सकते हैं, हमारी प्रस्तावित विधि बहुपद कार्यों को डेटा को एन्क्रिप्ट और डिक्रिप्ट करने की कुंजी के रूप में मानती है। प्रेषक और रिसीवर के बीच महत्वपूर्ण विनिमय हर सममित कुंजी एल्गोरिथ्म में पहला चरण है। हमारे पास कुंजी विनिमय करने का एक तरीका है। वास्तव में, उच्च डिग्री बहुपद का उपयोग ब्लॉक सिफर पर हमलों को कम करने के लिए किया जा सकता है, जो शास्त्रीय और साथ ही क्वांटम हमले के लिए सच है। निम्नलिखित एल्गोरिथम चरण हैं:

एल्गोरिथ्म 1. कुंजी उत्पत्ति का एल्गोरिथ्म

निवेश : n: कुंजी-बहुपद की डिग्री

आउटपुट : n+1 लंबाई का एक सारणी K (कुंजी-बहुपद)

चरण 1 : गुप्त कुंजी-बहुपद की डिग्री प्राप्त करने के लिए इनपुट 'n'

चरण 2 : i = 0 से n के लिए यादच्छिक बीज Vi का एक सेट उत्पन्न करें।

चरण 3 : रेंज [0 से n] में [i, Ki,] i की एक तालिका उत्पन्न करें।

चरण 4 : दोनों i और Ki

चरण 5 : इच्छित प्राप्तकर्ता को Ki भेजें / भौतिक कुंजी शेयर

चरण 6 : कुंजी-बहुपद 'n' की डिग्री भेजें

चरण 7 : अंत के लिए

चरण 8 : कुंजी-बहुपद = n+1 लंबाई के K की सारणी

चरण 9 : कुंजी तालिका को युग्म कुंजी-तालिका [रिसीवर-आईडी, K सारणी] के रूप में बनाए रखें

एल्गोरिथ्म 1 एक सुरक्षित भौतिक माध्यम में बहुपद के सह-कुशल और डिग्री को स्थानांतरित करने के तरीके को चित्रित कर रहा है। इन सह-कुशल मानों का उपयोग समीकरण (2) में दिए गए अनुसार कुंजी-बहुपद उत्पन्न करने के लिए किया जाएगा।

कुंजी-बहुपद = $\{K_n X^n + K_{n-1} X^{n-1} ....+ K_0 X^0\} = K_0 + K_1 X^1 + K_2 X^2 + ...+ K_n X^n$ ..... (2)

कुंजी की स्थापना के बाद, अगला कदम दिए गए संदेश को सिफर टेक्स्ट में एन्क्रिप्ट करना है। संदेश की लंबाई n+1 सारणी के समान रूप में है। सबसे पहले, संदेश एमआई का जोड़ प्रमुख तत्व की के साथ किया जाता है, और नई सारणी संग्रहीत की जाती है, उस सारणी को सिफर बहुपद के रूप में काम किया जाता है। इसके बाद, जड़ों के लिए नया बहुपद हल किया जाता है। बहुपद की सभी जड़ों को खोजने के लिए एक उपयुक्त विधि का उपयोग किया जाता है। सभी जड़ों को खोजने के बाद रूट सारणी उत्पन्न होती है और यह रूट सारणी सिफर टेक्स्ट है जिसे प्रेषित किया जा रहा है। एन्क्रिप्शन की प्रक्रिया एल्गोरिथ्म 2 में परिभाषित की गई है।

एल्गोरिथ्म 2. बहुपद कुंजी का उपयोग करके एन्क्रिप्शन

निवेश : कुंजी-बहुपद K और संदेश सारणी M, दोनों सरणियों की लंबाई n+1 है।

आउटपुट : साइफर सारणी R

चरण 1 : मुख्य बहुपद है: KP = K0 + K1X1 + K2X2 + ... + KnXn

सारणी में मुख्य बहुपद K={K 0, K1, K2 ....., Kn } है।

चरण 2 : संदेश सारणी है: M={M0, M1, M2 ....., Mn}

चरण 3 : एक्सओआर द्वारा संदेश ब्लॉक को किसके

साथ जोड़कर नया सिफर बहुपद उत्पन्न करें

दिए गए कुंजी बहुपद के गुणांक:

CT = (M0 ⊕K 0)X0 +(M1 ⊕K1)X1 + (M2 ⊕K2) X2 + ... + (Mn ⊕Kn)Xn

चरण 4 : C = {M0 ⊕K0, M1 ⊕K1,, M2 ⊕K2,....., Mn ⊕Kn} (सिफर संदेश सारणी)

चरण 5 : एक उपयुक्त विधि द्वारा इस सिफर संदेश बहुपद की सभी जड़ों का पता लगाएं और इसे रूट

सारणी में संग्रहीत करें

चरण 6 : रूट सारणी R = {R1, R2, ..., Rn} है।

चरण 7 : रूट सारणी को रिसीवर को सिफर टेक्स्ट के रूप में भेजें

एल्गोरिथ्म 3 में, डिक्रिप्शन प्रक्रिया को समझाया गया है, जड़ों का एक सेट सिफर सारणी के रूप में एक रिसीवर द्वारा प्राप्त किया जाएगा। प्रेषक द्वारा उपयोग किए जाने वाले बहुपद को पुनर्जीवित करने के लिए जड़ों का एक सरल गुणन किया जाता है। प्राप्त बहुपद को रिसीवर के साथ पहले से साझा किए गए गुप्त बहुपद के साथ आगे संसाधित किया जाना चाहिए। सह-कुशल को एक सरल एक्सओआर करने से मूल बहुपद को पुनर्जीवित किया जाएगा जिसमें सभी सह-कुशल हैं जो बदले में मूल सादा संदेश है।

एल्गोरिथ्म 3. डिक्रिप्शन एल्गोरिथ्म

निवेश : R से सिफर, कुंजी-बहुपद K

आउटपुट : संदेश सारणी M

चरण 1 : सिफर सारणी R={R1, R2, R3, ...Rn} है।

चरण 2 : मूल समीकरण को गुणा करके एक बहुपद उत्पन्न करें।

P=(X-R1) * (X-R2) * (X-R3) *..... * (X-Rn)

चरण 3 : परिणामी बहुपद

P= C0X0 + C1X1 + C2X2 + ... + CnXn

चरण 4 : सादा संदेश प्राप्त करने के लिए कुंजी-बहुपद के साथ XORing

TP = (C0 ⊕K0)X0 +(C1⊕K1)X1 + (C2 ⊕K2)X2 + ... + (Cn ⊕Kn)Xn

चरण 5 : प्राप्त गुणांक सारणी है: M = {M0, M1, M2 ....., Mn}

चरण 6 : सारणी M प्राप्तकर्ता के लिए आवश्यक संदेश है।

M ={M0, M1, M2 ....., Mn} की सारणी में सभी सादे संदेश हैं, प्रारंभिक क्रम परिवर्तन और संयोजनों का उपयोग करके सारणी आधारित भ्रम और प्रसार के साथ एक ही प्रक्रिया को बढ़ाया जा सकता है।

निष्कर्ष और भविष्य के काम

ब्लॉक सिफरिंग हमेशा स्टीम सिफर पर क्रिप्टोग्राफी का एक पसंदीदा तरीका है क्योंकि उनके तेजी से निष्पादन, कम विलंबता और कम मेमोरी आवश्यकताओं के कारण। एईएस एक मानक है जो एक समय में **16** बाइट से **32** बाइट के ब्लॉक को एन्क्रिप्ट कर सकता है और इसे हाल के वर्षों में एक मानक एल्गोरिदम के रूप में जाना जाता है और इसका उपयोग कई डिजिटल अनुप्रयोगों के लिए किया जा रहा है। हालांकि, यह तीन प्रमुख मानक आकारों **128,192** एवं **256** में काम कर रहा है। हमलावर हमला करने के लिए शास्त्रीय और क्वांटम तकनीक दोनों का उपयोग कर सकता है। यह मुख्य सीमा निश्चित-कुंजी आकार एन्क्रिप्शन एल्गोरिदम है। हमने बहुपद का उपयोग करके डेटा एन्क्रिप्ट करने की एक नई विधि का प्रस्ताव दिया है, जिसमें पेलोड को एन्क्रिप्ट और डिक्रिप्ट करने के लिए एक चर आकार की कुंजी रखने का प्रावधान है। प्रस्तावित एल्गोरिथ्म का मुख्य विचार दिए गए बहुपद के सह-कुशल में पेलोड को छिपाने के लिए दो बहुपदों का उपयोग करना है। एक गुप्त बहुपद के साथ सभी जड़ों और एक्सओरिंग की खोज फिर से सादे संदेश को वापस लाएगी। इस प्रस्ताव में निम्नलिखित फायदे हैं: परिवर्तनीय ब्लॉक सिफर, चर कुंजी लंबाई, कुंजी-आकार आधारित हमलों को कम करना, तेज और विश्वसनीय। हालांकि, किसी दिए गए

बहुपद की सभी जड़ों की खोज करने और काल्पनिक जड़ों से निपटने के लिए अभी भी कुछ चुनौतियां हैं। कुल मिलाकर, हमने क्रिप्टोग्राफी एल्गोरिदम के लिए कुंजी के रूप में बहुपद का उपयोग करने का प्रस्ताव दिया है जो क्रिप्टोग्राफिक डोमेन के लिए नए तरीके खोलता है।

संदर्भ:

[N1] - डिफी, डब्ल्यू, और हेलमैन, एम (1976)। क्रिप्टोग्राफी में नई दिशाएं। सूचना सिद्धांत पर आईईईई लेनदेन, 22 (6), 644-654।

[N2] - ठाकुर, जे, और कुमार, एन (2011)। डीईएस, एईएस, और ब्लोफिश: सममित कुंजी क्रिप्टोग्राफी एल्गोरिदम सिमुलेशन आधारित प्रदर्शन विश्लेषण। उभरती हुई प्रौद्योगिकी और उन्नत इंजीनियरिंग की अंतर्राष्ट्रीय पत्रिका, 1 (2), 6-12।

[N3] - अल-शबी, एमए (2019)। सूचना सुरक्षा में सममित और असममित क्रिप्टोग्राफी एल्गोरिदम पर एक सर्वेक्षण। इंटरनेशनल जर्नल ऑफ साइंटिफिक एंड रिसर्च पब्लिकेशंस (आईजेएसआरपी), 9 (3), 576-589।

[N4] - बर्नस्टीन, डीजे, और लैंग, टी (2017)। पोस्ट-क्वांटम क्रिप्टोग्राफी। प्रकृति, 549 (7671), 188-194।

[N5] - चेन, एल., चेन, एल., जॉर्डन, एस., लियू, वाई.के., मूडी, डी., पेराल्टा, आर., ... स्मिथ-टोन, डी (2016)। पोस्ट-क्वांटम क्रिप्टोग्राफी पर रिपोर्ट (वॉल्यूम 12)। गैथर्सबर्ग, एमडी, यूएसए: यूएस डिपार्टमेंट ऑफ कॉमर्स, नेशनल इंस्टीट्यूट ऑफ स्टैंडर्ड एंड टेक्नोलॉजी।

[N6] - अलाजिक, जी., एल्पेरिन-शेरिफ, जे., एपोन, डी., कूपर, डी., डैंग, क्यू., केल्सी, जे., और स्मिथ-टोन, डी. (2020). एनआईएसटी पोस्ट-क्वांटम क्रिप्टोग्राफी मानकीकरण प्रक्रिया के दूसरे दौर पर स्थिति रिपोर्ट। अमेरिकी वाणिज्य विभाग, एनआईएसटी।

[N7] - बुचमैन, जे.ए., ब्यूटिन, डी., गोफर्ट, एफ., और पेट्ज़ोल्ड्ट, ए. (2016). पोस्ट-क्वांटम क्रिप्टोग्राफी: कला की स्थिति। नए कोडब्रेकर, 88-108।

[N8] - डिंग, जे, और पेट्ज़ोल्ट, ए (2017)। मल्टीवेरिएट क्रिप्टोग्राफी की वर्तमान स्थिति। IEEE सुरक्षा और गोपनीयता, 15 (4), 28-36.

[N9] - आर. एम. डेविस, "परिप्रेक्ष्य में डेटा एन्क्रिप्शन मानक," आईईईई संचार।, खंड 16, संख्या 6, पीपी 5-9, 1978, दोई: 10.1109 / MCOM.1978.1089771

[N10]- "डिजिटल हस्ताक्षर और सार्वजनिक कुंजी क्रिप्टोसिस्टम प्राप्त करने के लिए एक विधि," एसीएम के संचार, 21, सो 2, पीपी 120-126, 1978।

[N11]- हेलमैन, "गोपनीयता और प्रमाणीकरण: क्रिप्टोग्राफी का एक परिचय," प्रोक आईईईई, खंड 67, संख्या 3, पीपी 397-427, 1979, दोई: 10.1109 /

[N12]- जीजे सिमंस, "सममित और असममित एन्क्रिप्शन," एसीएम कम्प्यूट। सुर्व, खंड 11, संख्या 4, पीपी 305-330, 1979, दोई: 10.1145/356789.356793।

[N13]- एम.ई. स्मिड और डी. के. ब्रैनस्टैड, "डेटा एन्क्रिप्शन मानक: अतीत और भविष्य," प्रोक आईईईई, खंड 76, संख्या 5, पीपी 550-559, 1988, दोई: 10.1109/5.4441।

[N14] - मर्कल, एमई हेलमैन, "मल्टीपल एन्क्रिप्शन की सुरक्षा पर," संचार। एसीएम, वॉल्यूम 24 (7), पीपी 465-467 (1981)।

[N15]- लाइ और जेएल मैसी, "एक नए ब्लॉक एन्क्रिप्शन मानक के लिए एक प्रस्ताव," लेक्ट नोट्स कम्प्यूट। (सबसर लेक्ट नोट्स सहित) इंटेल। नोट्स जैव सूचना विज्ञान, खंड 473 एलएनसीएस, पीपी 389-404, 1991, दोई: 10.1007/3-540-46877-3_35।

[N16]- एम. अग्रवाल, "सममित कुंजी एन्क्रिप्शन

तकनीकों पर एक तुलनात्मक सर्वेक्षण," खंड 4, संख्या 05, पीपी 877-882, 2012।

[N17]- डेमेन और वी रिजमेन, "एईएस प्रस्ताव: रिजेंडेल," 1999।

[N18] - ई. जे. स्वांकोस्की, आर. आर. ब्रूक्स, वी. नारायणन, एम. कांडेमिर और एम. जे. इरविन, "सुरक्षित एफपीजीए सममित एन्क्रिप्शन के लिए एक समानांतर वास्तुकला"। प्रोक - इंटरनेशनल पैरेलल डिस्ट्रिब प्रक्रिया। IPDPS 2004 (सार CD-ROM), खंड 18, संख्या सी, पीपी 1803-1810, 2004, दोई: 10.1109 /

[N19] - के. कुमार, के. आर. रामकुमार और ए. कौर, "एफपीजीए पर उन्नत एन्क्रिप्शन मानक (एईएस) एल्गोरिथ्म का एक डिजाइन कार्यान्वयन और तुलनात्मक विश्लेषण"।ICRI-TO 2020 - IEEE 8 वीं अंतर्राष्ट्रीय सम्मेलन। इन्फोकॉम टेक्नोलॉजी। (रुझान भविष्य. निर्देशन.) पीपी। 182–185, 2020, दोई: 10.1109/ICRITO48877.2020.9198033.

[N20] - ई. एल. डी. डी. डी, "पब्लिक-की क्रिप्टोग्राफी के पहले दस साल," वॉल्यूम 76, नंबर 5, पीपी 560-577, 1988।

[N21] - कोब्लिट्ज़, ए मेनेज़ेस और एस वैनस्टोन, "द स्टेट ऑफ एलिप्टिक कर्व क्रिप्टोग्राफी," डेस। कोड, क्रिप्टोग्र., खंड 19, संख्या 2–3, पीपी 173-193, 2000, दोई: 10.1023 1008354106356/

[N22] - शोर, "क्वांटम गणना के लिए एल्गोरिदम: असतत लघुगणक और फैक्टरिंग," कंप्यूटर विज्ञान की नींव पर 35 वीं वार्षिक संगोष्ठी, 1994, पीपी 124-134, दोई: 10.1109 /

[N23] - ग्रोवर, "डेटाबेस खोज के लिए एक तेज़ क्वांटम मैकेनिकल एल्गोरिथ्म", कंप्यूटिंग के सिद्धांत पर अट्ठाईसवें वार्षिक एसीएम संगोष्ठी की कार्यवाही में, 1669, पीपी 212-219।

[N24] - "एक परिमित क्षेत्र पर समीकरणों के आधार पर एक सार्वजनिक-कुंजी क्रिप्टोसिस्टम," क्रिप्टोलॉजी, वॉल्यूम 7, नंबर 4, पीपी 347-358, 1983, दोई: 10.1080/0161-118391858071।

[N25] - R. लिडल, "बहुपद और परिमित क्षेत्रों के आधार पर क्रिप्टोसिस्टम पर," क्रिप्टोग्राफिक तकनीकों के सिद्धांत और अनुप्रयोग पर कार्यशाला, 1984, पीपी 10-15।

[N26]- एम नौर और बी पिंकास्ट, "बेखबर स्थानांतरण और बहुपद मूल्यांकन," कॉन्फ प्रोक अन्नू। एसीएम संगोष्ठी सिद्धांत कम्प्यूट।, पीपी 245–254, 1999, दोई: 10.1145/301250.301312।

[N27] - "बहुपद पुनर्निर्माण समस्या पर आधारित एक सार्वजनिक कुंजी एन्क्रिप्शन योजना," लेक्ट नोट्स कम्प्यूट साइंस। इंटेल। नोट्स जैव सूचना विज्ञान, खंड 2656, पीपी 229-240, 2003, दोई: 10.1007/3-540-39200-9_14।

[N28] - "यूरोक्रिप्ट 2003 में प्रस्तुत बहुपद पुनर्निर्माण आधारित क्रिप्टोसिस्टम की मरम्मत के लिए ट्रेस ऑपरेटर का उपयोग करना। आईएसीआर क्रिप्टोल। ईप्रिंट आर्क।, वॉल्यूम 2003, पी. 209, 2003, [ऑनलाइन]। उपलब्ध: http://dblp.uni-trier.de/db/journals/iacr/iacr2003.html#AugotFL03.

[N29] - "बहुपद पुनर्निर्माण समस्या के आधार पर एक सार्वजनिक-कुंजी एन्क्रिप्शन योजना का क्रिप्टैनालिसिस," लेक्ट नोट्स कम्प्यूट साइंस। इंटेल। जैव सूचना विज्ञान, खंड 2947, पीपी 14-27, 2004, दोई: 10.1007/978-3-540-24632-9_2।

[N30] - कियायस और एम युंग, "इष्टतम पैरामीटर विकल्प के तहत बहुपद-पुनर्निर्माण आधारित सार्वजनिक-कुंजी प्रणाली का क्रिप्टएनालिसिस," लेक्ट नोट्स कम्प्यूट साइंस। इंटेल। जैव सूचना विज्ञान, खंड 3329, पीपी 401-416, 2004, दोई: 10.1007/978-3-540-30539-2_28।

[N31] - एस. बी. सदखान और के. एच. रूमा, "लैग्रेंज प्रक्षेप विधि का उपयोग करके बहुपद पुनर्निर्माण समस्या का मूल्यांकन," पृष्ठ 1399-1403, 2006, दोई: 10.1109/

[N32] - घोष, ए., और साहा, ए. (2013). स्टेग्नोग्राफ़ी के साथ एक संख्यात्मक विधि आधारित एन्क्रिप्शन एल्गोरिथ्म। कम्प्यूट। विज्ञान प्रौद्योगिकी प्रौद्योगिकी, 3, 149-157।

[N33] - पी. सोनिया और एस. कुमार ग्रेवाल, "बहुपद एन्क्रिप्शन मानक का हैशिंग कुंजी आधारित विश्लेषण"। इंक. जे. कम्प्यूट. नेट। Inf. सुरक्षित करें।, खंड 8, संख्या 11, पीपी 44-51, 2016, दोई: 10.5815 / ijcnis.2016.11.05।

[N34] - अल-सियाक, "संख्यात्मक तरीकों पर आधारित सार्वजनिक कुंजी क्रिप्टोसिस्टम," खंड 13, संख्या 7, पीपी 3105-3112, 2017।

[N35] - चेओन, एस होंग, सी ली और वाई सोन, "रैखिक सिफरटेक्स्ट आकार के साथ बहुपद कार्यात्मक एन्क्रिप्शन योजना," पीपी 1-23, 2018।

[N36] - स्टोयानोव और जी नेडज़िबोव, "रोटेशन-अनुवाद समीकरण के आधार पर सममित कुंजी एन्क्रिप्शन," समरूपता (बेसल)।, वॉल्यूम 12, नंबर 1, पीपी 2-12, 2020, दोई: 10.3390/

[N37] - हेक्टेअर। फू, डेसकार्टेस के संकेतों के नियम के बारे में कुछ टिप्पणियां, एलिमेंट डेर मैथेमैटिक, 69 (2014), पीपी 186-194।

तीन-चरणीय दृष्टिकोण से क्षेत्रीय और भीड़ निगरानी में स्वार्म ड्रोन प्रणालियों का अधिगम

श्री हरीश कुमार, प्रविधिज्ञ 'ए'

परिचय

आज के समय में जहाँ लोगों और संसाधनों की पहुँच हर जगह है ऐसे समय में निरीक्षण और निगरानी पर विशेष ध्यान दिया जाना जरुरी है।

हमें क्षेत्रीय और भीड़ निगरानी एवं जाँच की जरुरत क्यूँ है?

संघ और क्षेत्र सर्विलांस की आवश्यकता कई व्यावसायिक और अक्सर महत्वपूर्ण कारणों से उत्पन्न होती है:

1. **सुरक्षा और निगरानी:** सर्विलांस व्यक्तियों की सुरक्षा सुनिश्चित करने में मदद करता है जो एक संघ या एक विशिष्ट क्षेत्र में होते हैं। यह अधिकारियों को संभावित खतरों की पहचान और त्वरित प्रतिक्रिया करने में सहायक सिद्ध होता है, जैसे कि आपराधिक गतिविधियों, आतंकवादी कार्रवाई, या हिंसक घटनाओं के मामले में।
2. **आपातकालीन प्रतिक्रिया:** सर्विलांस आपातकालीन समय में वास्तविक समय में जानकारी प्रदान करता है, जिससे पहली प्रतिक्रिया देने वाले व्यक्तियों को स्थिति को सटीकता से मूल्यांकित करने और संसाधनों को प्रभावी रूप से आवंटित करने में सहायक होता है। यह प्राकृतिक आपदाओं, दुर्घटनाओं और सार्वजनिक स्वास्थ्य संकटों में महत्वपूर्ण है।
3. **सीमा और समुद्री सुरक्षा:** सर्विलांस सीमाओं और समुद्र तटों की मॉनिटरिंग में मदद करता है, अवैध आप्रवासन, तस्करी, और अन्य खतरों को रोकने में।

वह प्रणालियाँ एवं उपकरण जिनका उपयोग वर्तमान में निरीक्षण और निगरानी के लिए किया जाता है –

1. क्लोज्ड सर्किट टेलीविजन (सी.सी.टी.वी.) कैमरे: स्थायी और गतिशील सीसीटीवी कैमरे राजनीतिक क्षेत्रों, सैन्य स्थापनाओं और महत्वपूर्ण बुनियादी ढांचाओं की निगरानी करने के लिए विशिष्ट रूप से रखे जाते हैं। वे निरंतर किसी निर्दिष्ट क्षेत्र में गतिविधियों की रिकॉर्डिंग प्रदान करते हैं।
2. **जीवमान निगरानी:** चेहरे की पहचान की तकनीक अवश्य किसी संघ में उपस्थित व्यक्तियों की पहचान करने के लिए उपयोग की जाती है। यह रक्षा अधिकारियों के लिए ज्ञात संदेह या दिलचस्प व्यक्तियों की पहचान करने में मदद कर सकती है।
3. **लिडार (लाइट डिटेक्शन एंड रेंजिंग):** लिडार प्रौद्योगिकी लेज़र बीम का उपयोग विस्तृत 3D मानचित्र बनाने के लिए करती है। यह भूमि की मैपिंग, वस्तु की पहचान और भूदृश्यों में परिवर्तनों की निगरानी के लिए उपयोग होती है।
4. **सैटलाइट छवियाँ:** उच्च-रिजॉल्यूशन की उपग्रह छवियाँ विशाल क्षेत्रों की व्यापारिक दृष्टि से पूरी दिखाई देती हैं, जो रक्षा बलों की गतिविधियों की निगरानी, परिवर्तनों की पहचान और संभावित सुरक्षा संदेहों के मूल्यांकन में मदद करती है।
5. **थर्मल इमेजिंग कैमरे:** ये कैमरे गरमी की साख दर्शाते हैं, जिनसे कम प्रकाश या बर्फीले मौसम की स्थितियों में निगरानी की जा सकती है। इनसे गरमी उत्सर्जित करने वाले व्यक्तियों या वस्तुओं की पहचान की जाती है।
6. **ध्वनिक सेंसर:** ध्वनिक सेंसर आवाजों की पहचान और विश्लेषण कर सकते हैं, जिससे गोलियों, विस्फोटों या अन्य असामान्य श्रवण पैटर्न की पहचान हो सकती है।
7. **ड्रोन स्वार्म:** कई ड्रोन्स को समन्वयित रूपों में साथ में कार्य करने के लिए उपयोग किया जा सकता है, जो निगरानी क्षमताओं को बढ़ावा देते हैं, बड़े क्षेत्रों की निगरानी करने में मदद करते हैं तथा स्थितिगत जागरूकता बढ़ाते हैं। इन सभी तकनीकों एवं प्रणालियों में से ड्रोन स्वार्म ही ऐसी आधुनिक प्रणाली है जो कि बड़ी संख्या में संसाधनों का इस्तेमाल बहुत कुशलता पूर्वक कर सकती है।

स्वार्म ड्रोन प्रणाली

स्वार्म ड्रोन अपने आप में एक इकलौती प्रणाली नहीं है बल्कि यह बहुत सारी प्रणालियों का मिश्रण है।

1. **अणुविधानित नियंत्रण:** स्वार्म में प्रत्येक ड्रोन स्वतंत्र रूप से काम करता है और सरल नियमों का पालन करता है, जो आमतौर पर पड़ोसी ड्रोन के साथ स्थानीय इंटरैक्शनों पर आधारित होते हैं। यहाँ एक सेंट्रल नियंत्रक को आदेश देने की बजाय ड्रोन को समूह के साथ मिलकर लक्षित कार्रवाई को पूरा करने के लिए प्रोग्राम किया जाता है।
2. **संचार:** ड्रोन्स, साथी-ड्रोन से जानकारी साझा करने, डेटा आदान-प्रदान करने, और अपने कार्रवाइयों को समन्वयित करने के लिए संवाद करते हैं। इसे वायरलेस संवादन या अन्य तरीकों से प्राप्त किया जा सकता है।
3. **वितरित एल्गोरिदम्स:** एल्गोरिदम तैयार किए जाते हैं ताकि रोबोट स्वार्म अपने आस-पास के वातावरण से जुड़ी जानकारी और अन्य ड्रोन के साथ इंटरैक्शन से निर्णय ले सकें।
4. **उत्पन्न व्यवहार:** व्यक्तिगत ड्रोन के संवादनों के परिणाम स्वरूप जटिल स्वार्म व्यवहार उत्पन्न होते हैं। ये व्यवहार समूह के लक्ष्यों की प्राप्ति में सहायक हो सकते हैं, जैसे कि खोज, मानचित्रण या पैटर्न बनाना।
5. **ड्रोन संवेदना:** ड्रोन अपने पर्यावरण को और अन्य ड्रोन की उपस्थिति को प्राप्त करने के लिए कैमरों, प्राक्सिमिटी सेंसर्स, या एक्सेलरोमीटर्स जैसे विभिन्न सेंसर्स का उपयोग करते हैं।
6. **पथ नियोजन:** ड्रोन अपने पथों का निर्धारण अपनी स्थिति, पड़ोसी ड्रोन की स्थिति, और स्वार्म के सामान्य लक्ष्य को मध्यस्थित करके करते हैं।
7. **स्वयं-संगठन:** स्वार्म ड्रोन में स्वयं-संगठन की जाती है, जहाँ ड्रोन बदलते पर्यावरण और अन्य ड्रोन की उपस्थिति के आधार पर अपने व्यवहार को समायोजित करते हैं, बिना किसी केंद्रीय निर्णयकर्ता की सहायता के।

इसी प्रकार मल्टी ड्रोन प्रणाली भी अलग अलग तकनीक का मिश्रण है।

1. **वितरित कार्य आवंटन:** ड्रोन कार्यों को अपनी क्षमताओं, कार्य के निकटबद्धता, और काम के बोझ के आधार पर अपने आप में वितरित करते हैं। इसमें अन्वेषण, मानचित्रण, निगरानी, और खोज जैसे कार्य शामिल हो सकते हैं।
2. **संचार:** ड्रोन के बीच प्रभावी संवादन, जानकारी साझा करने, डेटा आदान-प्रदान करने, और कार्रवाई की समन्वयन के लिए महत्वपूर्ण है। संवादन वायरलेस नेटवर्क्स या सीधे परस्पर प्रभावनों के माध्यम से हो सकता है।
3. **सहयोगी मानचित्रण और स्थानांतरण:** ड्रोन अपने स्थानीय मानचित्र और स्थानिक जानकारी को एक दूसरे के साथ साझा करके वातानुकुलित वातानुकुलन और वातानुकुलन मानचित्र को बनाने के लिए करते हैं।
4. **कार्य विभाजन और समन्वय:** मल्टी - ड्रोन प्रणालियों में अक्सर जटिल कार्यों को छोटे उप-कार्यों में विभाजित किया जाता है जिन्हें विभिन्न ड्रोन समय-समय पर करते हैं। प्रभावी समन्वय सुनिश्चित करता है कि उप-कार्य संयोजनीय तरीके से किए जा रहे हैं।
5. **स्वार्म इंटेलिजेंस तकनीकें:** कुछ मल्टी - ड्रोन प्रणालियाँ स्वार्म इंटेलिजेंस के सिद्धांतों से प्रेरित होती हैं, जैसे कि एंट कॉलोन ऑप्टिमाइजेशन या पार्टिकल स्वार्म ऑप्टिमाइजेशन, जिनका संयुक्त रूप से जटिल समस्याओं का समाधान होता है।
6. **केंद्रीय या वितरित नियंत्रण:** आवेदन के आधार पर, मल्टी- ड्रोन प्रणालियों में केंद्रीय नियंत्रण हो सकता है (जहां एक केंद्रीय एकत्रितता योजना के रूप में ड्रोन का प्रबंधन करता है) या वितरित नियंत्रण हो सकता है (जहां ड्रोन अपने खुद के अवलोकन और सीमित संवाद के आधार पर निर्णय लेते हैं)।
7. **संसाधन साझाकरण:** मल्टी-ड्रोन प्रणालियाँ संसाधनों के उपयोग के आदान-प्रदान को सुधारने के लिए संसाधनों का उपयोग कर सकती है, जैसे कि ऊर्जा, संवेदन क्षमताएँ तथा गणना शक्ति।
8. **गड़बड़ी सहिष्णुता और पुनरावलोकन:** मल्टी - ड्रोन प्रणाली में, अगर एक ड्रोन असफल होता है या मुश्किलों का सामना करता है, तो दूसरे रोबोट कार्य को जारी रख सकते हैं एवं सिस्टम की मजबूती बढ़ाते हैं।
9. **कार्य आवंटन एल्गोरिदम्स**: ये एल्गोरिदम्स रोबोट की क्षमताओं, कार्य की आवश्यकताओं, और प्रदर्शन की दिशा में उल्लिखित विचारों को ध्यान में

रखकर तय करते हैं कि कौन सा रोबोट कौन सा काम करेगा।

10. **पथ योजना और संघटन बचाव:** मल्टी - ड्रोन प्रणालियों को पथ योजना को प्रभावी बनाने और पर्यावरण में ड्रोन और बाधाओं के बीच संघटन को बचाने के लिए सक्षम होना चाहिए।

11. **सहयोगी परिप्रेक्ष्य:** ड्रोन संघ को वायवीय डेटा और अवलोकन साझा करने के लिए अपने संवेदना डेटा और अवलोकन साझा करते हैं ताकि पर्यावरण की अधिक सटीक और पूर्ण समझना मिल सके।

यह दोनों प्रणालियाँ अपने निर्धारित कार्य को कुशलता के साथ पूरा करती हैं लेकिन दोनो के कार्य करने की प्रणालियाँ काफी मिलती हैं एक विभिन्नता जो दोनों प्रणालियों को अलग करती है वह है स्वयं-संगठन, स्वार्म ड्रोन प्रणाली स्वयं-संगठन में सक्षम होती है वहीं दूसरी तरफ मल्टी रोबोटिक प्रणाली संगठन के प्रबंधन और बदलाव के लिए अपने केन्द्रीय सर्वर पे निर्भर होती है लेकिन अगर इन दोनों प्रणालियों के कुछ खास गुणों को मिलाया जाए तो यह प्रणाली निरीक्षण एवं निगरानी के दृष्टिकोण से बहुत प्रभावशाली सिद्ध हो सकती हैं।

तीन-चरणीय दृष्टिकोण

इस प्रस्ताव की अवधारणा केन्द्रीय प्रबंधन पर आधारित है लेकिन इसे तीन चरणों में विभाजित किया गया है।

चरण 1: केन्द्रीय सर्वर

उद्देश्य : इस चरण का उद्देश्य सभी गणितीय रूप से भारी कम्प्यूटेशनल और कठिन प्रक्रियाओं को संभालना है इस चरण में केन्द्रीय सर्वर या फिर उसी के बराबर का कोई संसाधन कार्य करेगा।

तरीका : इस चरण में उपस्थित सभी संसाधन दो तरह के संचार साधन (रेडियो तरंगे एवं वाई फाई) का उपयोग करेंगे तथा जी.पी.एस./जी.आई.एस. से एकत्रित सूचना का इस्तेमाल करेंगे एक स्पष्ट/अस्पष्ट धरना का निर्माण करने के लिए ताकि वह अपने उदेश्य को पूर्ण करने के लिए परियोजना तैयार कर सके जिसमें कि स्वार्म को छोटे झुंड में तोड़ना भी शामिल है इसके अलावा केन्द्रीय सर्वर यह भी सुनिश्चित करेगा की अभी तक कितना कार्य पूर्ण हुआ है और कितना शेष है तथा जल्द से जल्द यह निश्चित करेगा कि आगे कार्य करने के लिए रणनीति बदलना जरुरी है या नहीं।

महत्व : मूलत: इस चरण में उपयोग होने वाले संसाधन उच्च स्तर के निर्णय लेने, मिशन योजना, संसाधन आवंटन और रणनीतिक तैयारी के लिए जिम्मेदार है। केंद्रीय सर्वर विभिन्न स्रोतों से जानकारी प्रोसेस करता है, ताकि स्वार्म के व्यवहार का मार्गदर्शन करने के लिए निर्णय लिया जा सके।

चरण 2: क्लीन ड्रोन

प्रणाली में संचार का आधार: इस प्रणाली में संचार के लिए तीन तरह के संचार साधनों का उपयोग किया गया है जो कि इस प्रकार है -

रेडियो तरंगे- रेडियो तरंगो के कुछ विशेष गुण (दायरा, कम लेटेंसी, कम प्राकृतिक अवरोधन) इस संचार माध्यम को आदेश और निरीक्षण के लिए बहुत ही उपयोगी बनाते हैं LoRaWAN रेडियो तरंगो की ईएसआई तकनीक है जो की लम्बी दूरी कम से कम पर्यावरणिक आघात के साथ संचालित कर सकती है, यह सुनिश्चित करेगी की केन्द्रीय सर्वर के कमांड निर्देश क्लीन ड्रोन के पास ज्यादा से ज्यादा सटीकता के साथ पहुँच जाएँ।

वाई फाई (वायरलेस फिडेलिटी) - वाई फाई रेडियो तरंगो का एक आरक्षित रेडियो फ्रीक्वेंसी बैंड है जो की उच्च आवृत्ति के साथ कार्य करती है अर्थात इसमें जानकारी संचारित करने की गति तेज़ होती है इस तकनीक का प्रयोग ऐसी जानकारी को संचारित करने के लिए किया जायेगा जो आकार में बड़ी होगी उदाहरण के लिए एजेंट ड्रोन द्वारा ली गयी तस्वीरें या फिर क्लीन ड्रोन द्वारा जोड़ा हुआ और संसाधित की हुए जानकारी, इस तरह की जानकारी का संचार किसी तेज़ गति के माध्यम से ही किया जाना चाहिए वाई फाई तेज़ गति तो देता है लेकिन इसकी आवृत्ति ज्यादा होने की वजह से इसके संचार की सीमा कम है इस लिए इसे सिर्फ एजेंट ड्रोन से क्लीन ड्रोन और क्लीन ड्रोन से केन्द्रीय सर्वर पे जानकारी संचारित करने लिए प्रयोग किया जाएगा।

एन.एफ.सी. (नियर फील्ड कम्युनिकेशन) – यह प्रौद्योगिकी सिस्टम में सबसे निम्न सीमा वाली होगी, यह केवल एजेंट ड्रोन्स के साथ स्थानिक संवाद की स्थापना के लिए प्रयुक्त की जाएगी, संसाधन स्थितियों, सदस्य विवरण और जनगणना डेटा साझा करने के लिए ताकि त्वरित प्रेषण के लिए।

1. प्रारंभीकरण:

- सभी तीन चरणों के साधन सक्रिय किये जाते हैं व संचार माध्यम स्थापित करने से पहले एक पॉवर ऑन सेल्फ टेस्ट हर एक साधन द्वारा अपने हार्डवेयर

की जांच के लिए तथा एकत्रित जानकारी को मेमोरी में संरक्षित करने के लिए चलाया जाता है ।

- इसके बाद सभी तरह के संचार माध्यम स्थापित किये जाते हैं और उनका परीक्षण भी किया जाता है इस प्रक्रिया में जो भी जानकारी एकत्र होती है वह केन्द्रीय सर्वर के पास संरक्षित की जाती है।
- केंद्रीय सर्वर स्वार्म मिशन का प्रारंभ करता है, उद्देश्य सेट करता है, और सेल्फ टेस्ट के समय इकट्ठा की हुई जानकारी के आधार पर संसाधनों का आवंटन क्षेत्रों में करता है।

2. केंद्रीय सर्वर के निर्णय

- प्रारंभीकरण के पश्चात् केन्द्रीय सर्वर कुछ समय के बाद एकत्रित जानकारी की जाँच करता है और अपनी आधारभूत रणनीतियों की जाँच करता है और मिशन उद्देश्यों को प्रोसेस करता है।
- उच्च स्तर के निर्णय लेता है, जैसे कि मिशन प्राथमिकताएँ, फॉर्मेशन समायोजन, और संसाधन आवंटन।
- स्वार्म के लिए मिशन योजनाएँ और रणनीतियों को तैयार करता है।
- जी.पी.एस./ जी.आई.एस. अथवा अन्य बाहरी साधनों से मिली जानकारी को संशोधित कर के क्षेत्रीय जानकारी के साथ एजेंट ड्रोन द्वारा एकत्र की हुए जानकारी को सत्यापित करना।

3. संचार और कमांड रिले

- केंद्रीय सर्वर योजनाएँ, कमांड्स, और संसाधन आवंटन जानकारी को क्वीन ड्रोन्स को भेजता है। क्वीन ड्रोन इस जानकारी को एजेंट ड्रोन्स के साथ सत्यापित करती है।
- क्वीन ड्रोन ने आदेश और संसाधन आवंटन विवरण को अपने क्षेत्र के एजेंट ड्रोनों को भेजा और संविदान किया।
- एजेंट ड्रोन अपने क्वीन ड्रोन से कमांड प्राप्त करते हैं और उसे स्वीकार करते हैं।
- एजेंट ड्रोन्स क्लस्टर का आधार स्वार्म संगठन के तथ्य पे आधारित होता है।

4. स्थानीय निर्णय निर्माण (एजेंट ड्रोन)

- एजेंट ड्रोन अपने सेंसरों से डेटा एकत्र करते हैं, स्थानीय शर्तों का विश्लेषण करते हैं, और रियल टाइम में निर्णय लेते हैं।
- निर्णय आवरण में अवरोध टालने, पथ समायोजन करने, और स्थानीय फॉर्मेशन बनाए रखने जैसे निर्णय शामिल हो सकते हैं। जो की क्लस्टर को दिए गये क्षेत्र पे आधारित होंगे और इनका अध्ययन सेन्सस एल्गोरिदम और वितरित एल्गोरिदम्स के द्वारा किया जायेगा।
- एजेंट ड्रोन अपने क्वीन ड्रोन से प्राप्त किए गए कमांडों का स्थानीय निर्णय निर्माण करते हैं।
- एजेंट ड्रोन अपने वातावरण के अनुकूल ढलने के लिए गठन में बदलाव करते हैं और किसी बड़े बदलाव से पहले क्वीन ड्रोन से अनुमति की मांग करते हैं।
- एजेंट ड्रोन्स क्लस्टर का आधार स्वार्म संगठन के तथ्य पे आधारित है तो यह छोटे एजेंट ड्रोन क्लस्टर्स अपने कार्य को पूर्ण करने के लिए उत्तम व्यवहार का प्रदर्शन कर सकते हैं।

5. अनुकूलनात्मक निर्णय (क्वीन ड्रोन)

- क्वीन ड्रोन एजेंट ड्रोनों से प्रतिक्रिया प्राप्त करते हैं, उसे सेंसर्स डेटा के साथ मिलाकर केंद्रीय सर्वर के निर्णयों के साथ प्रोसेस करते हैं।
- क्वीन ड्रोन एजेंट ड्रोन्स के विभिन्न क्लस्टर से प्राप्त संगठन के बदलाव के अनुरोध को जांचती है तथा केन्द्रीय सर्वर से प्राप्त निर्देशों के साथ उन अनुरोधों का अध्ययन कर के स्वीकार या अस्वीकार करती है।

6. डेटा फ्यूज़न और विश्लेषण

- एजेंट ड्रोन स्वच्छंद दृष्टिकोण से सर्विलांस डेटा एकत्र करते हैं।
- क्वीन ड्रोन एजेंट ड्रोनों से डेटा प्राप्त करते हैं और डेटा फ्यूज़न करते हैं ताकि निगरानी क्षेत्र का एक व्यापक प्रतिष्ठान बना सकें।
- फ्यूज्ड् डेटा को अगले विश्लेषण और रिपोर्टिंग के लिए केंद्रीय सर्वर को भेजा जाता है।

7. प्रतिक्रिया और रिपोर्टिंग

- क्वीन ड्रोन अपनी क्लस्टर की स्थितियों, फॉर्मेशन समायोजन, और स्थानीय अवरोधों की रियल टाइम प्रतिक्रिया प्रदान करते हैं।

- केंद्रीय सर्वर क्वीन ड्रोनों से प्रतिक्रिया प्राप्त करता है, जिससे स्वार्म के प्रदर्शन की समग्र अवधारणा की जा सकती है।

8. मिशन निष्पादन और अनुकूलन

- स्वार्म मिशन कार्यों को सामूहिक रूप से निष्पादित करता है, पर्यावरण और मिशन प्रयोजनों में परिवर्तनों का अनुकूलन करता है।
- क्वीन ड्रोन रियल टाइम प्रतिक्रियाओं के आधार पर फॉर्मेशन और रणनीतियों को समायोजित करना जारी रखते हैं।

9. मिशन पूरा होना

- मिशन उद्देश्य सर्वेलन्स डेटा का एकत्र करने और उसके लक्ष्यों को प्राप्त करने के साथ पूरे होते हैं।
- केंद्रीय सर्वर क्वीन ड्रोन्स से अंतिम डेटा प्राप्त करता है, जिससे पोस्ट-मिशन विश्लेषण और रिपोर्टिंग की जा सकती है।

लाभ

- तीन स्तरीय संरचना निर्णय प्रवाह की कुशलता सुनिश्चित करती है।
- स्थानीय निर्णय लेना गतिशील वातावरण के प्रति अनुकूलन को बढ़ावा देते हैं।
- क्वीन ड्रोन स्तर पर अनुकूलन के निर्णय क्लस्टर के व्यवहार को अद्यतन करते हैं।
- डेटा फ्यूजन वास्तविक स्थिति जागरूकता प्रदान करता है।
- केंद्रीय सर्वर उच्च स्तर की रणनीति निर्माण और संसाधन आवंटन की स्थानीय व्यवस्था को संभालता है।

चुनौतियाँ

- सभी स्तरों पर संवाद और समक्रिया को सुनिश्चित करने के लिए अद्वितीय संवाद और समक्रिया व्यवस्था।
- फॉर्मेशन नियंत्रण, अवरोध टालने, और स्थानीय निर्णय निर्माण के लिए मजबूत एल्गोरिदम विकसित करना।
- रियल टाइम निर्णय लेने में विलंब और बैंडविड्थ समस्याओं का समाधान।
- संसाधन की गुणवत्ता, अनिश्चितता, और संग्रहण समस्याओं का समाधान करना।

यह कार्यप्रवाह केंद्रीय सर्वर, क्वीन ड्रोनों, और एजेंट ड्रोनों के बीच कैसे इंटरैक्ट करते हैं, कोऑर्डिनेटेड सर्विलांस कार्यों को प्राप्त करने के लिए और समग्रता प्राप्त करने के लिए दिखाता है। असली कार्यप्रवाह कार्यों की जटिलता, संचार ढांचा व उनकी विशिष्ट तकनीकी चुनौतियों पर निर्भर करेगा।

सिमुलेशन परिणाम और विश्लेषण

ये परिणाम चित्रात्मक हैं और आप्पके विशिष्ट सिमुलेशन सेटअप और उद्देश्यों के अनुसार विविधता दिलाने के लिए बनाए जा सकते हैं।

सिमुलेशन परिदृश्य:

लक्ष्य: एक बड़े क्षेत्र की निगरानी

सिमुलेट किये जाने वाले लक्ष्य: एजेंट ड्रोन की अपने वातावरण के अनुसार संगठन में बदलाव के सुझाव की क्षमता।

संख्या (एजेंट ड्रोनों एवं क्वीन ड्रोन): 64 एवं 4

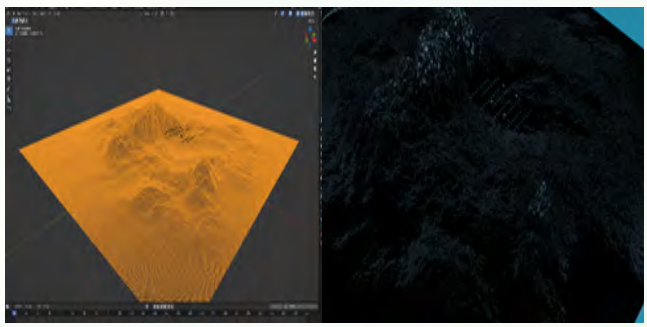
तोड़े जाने वाले क्लस्टर: 4

मूलभूल संगठन की संरचना: मेश संरचना

प्रारंभिक आदर्श जानकारी: प्रयुक्त मानचित्र के सटीक निर्देशांक और ऊंचाई मानचित्र

एजेंट ड्रोन सेंसर्स: आई आर सेंसर , अल्ट्रा सोनिक सेंसर, कैमरा

उपयोग किये गये मानचित्र का ऊंचाई जानकारी के आधार पे चित्रण (केन्द्रीय सर्वर पे बनी हुए छवि) चमकते बिंदु ड्रोनस की स्थिति दर्शाते हैं।



सिमुलेशन प्रारंभ:

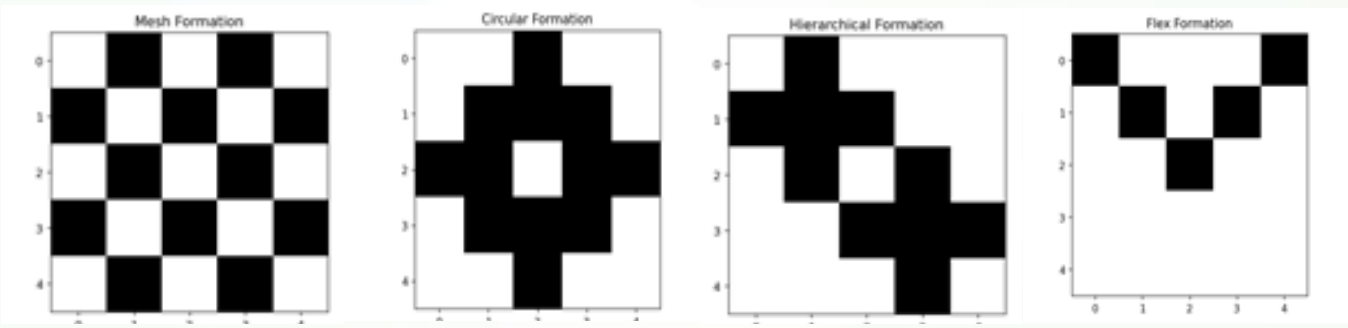
- मेश संगठन के बाद स्वार्म को क्षेत्र की निगरानी के लिए 4 भागों में विभाजित किया गया, प्रारंभिक स्थानीय सेंसर्स की जानकारी के आभाव में सिर्फ जी.पी.एस. जानकारी के आधार पर ड्रोन स्वार्म ग्रेडिएंट नविगेशन एल्गोरिदम (परिमाप: ऊंचाई) का उपयोग करते हुए क्लस्टर्स को उनके क्षेत्रों की जानकारी दे दी गयी।

- हर एक एजेंट ड्रोन के पास 2 प्रकार के यूनिक आई.डी. कोड हैं जो उसकी पहचान स्वार्म और मानचित्रण के ढांचे में करता है दूसरा कोड जो की उसकी पहचान स्थानीय क्लस्टर के सदस्य के रूप में करता है क्लस्टर के बनने के बाद हर एक क्लस्टर डिस्ट्रिब्यूटेड एल्गोरिदम, सेन्सस एल्गोरिदम, टोकन एल्गोरिदम और सेल्फ फॉर्मेशन एल्गोरिदम का इस्तेमाल करने लगे। (केवल गठन सेल्फ फॉर्मेशन के एल्गोरिदम को ही पूर्व ट्रेन किया गया है शेष सभी एल्गोरिदम नियम पर आधारित दृष्टिकोण का प्रयोग करते हैं)
- क्वीन ड्रोन्स अपने अपने क्लस्टर के एजेंट्स ड्रोन्स से उनकी स्थिति, संसाधन और सेंसर्स से एकत्र किये गये जानकारी का फ्यूज़न करने लगी तथा यह जानकारी केन्द्रीय सर्वर को संचालित कर दी गयी।
- एजेंट ड्रोनों से डेटा को क्वीन ड्रोन के द्वारा मिलाकर, एक व्यापक निगरानी क्षेत्र का प्रतिष्ठान बनाया जाता है।

अनुकूलनात्मक व्यवहार

एजेंट ड्रोन्स रियल टाइम जानकारी एकत्रित करके अपने अपने फॉर्मेशन के अध्ययन करने लगे, सेन्सर्स एल्गोरिदम की सहायता से हर एक क्लस्टर ने अपने क्षेत्र के अनुरूप एक प्रारंभिक फॉर्मेशन का निर्माण किया।

क्लस्टर	फॉर्मेशन	क्षेत्र
क्लस्टर 1	मेश फॉर्मेशन	कम ऊंचाई वाले क्षेत्र
क्लस्टर 2	सर्कुलर फॉर्मेशन	मध्यम ऊंचाई वाले क्षेत्र
क्लस्टर 3	पदानुक्रम फॉर्मेशन	मध्यम ऊंचाई वाले क्षेत्र
क्लस्टर 4	फ्लेक्स फॉर्मेशन	अधिक ऊंचाई वाले क्षेत्र



(काले क्षेत्र क्लस्टर में ड्रोनस की एक अनुमानित स्थिति है)

क्वीन ड्रोन एजेंट ड्रोन्स की प्रतिक्रियाओं और केंद्रीय सर्वर के इनपुट्स के आधार पर अनुकूलनात्मक निर्णय लेते हैं। क्वीन ड्रोन के पास निगरानी वाले क्षेत्र और उस क्षेत्र में उपस्थित क्लस्टर के गठन की जानकारी रहती है जिसके आधार पे क्वीन ड्रोन उस क्षेत्र के लिए उपयोगी फॉर्मेशन का अनुमान लगाती है और यह देखती है की क्लस्टर द्वारा तय की गयी रणनीति क्वीन ड्रोन द्वारा तय की गयी रणनीति से कितने प्रतिशत मेल खाती है। परिस्थितियों में बदलाव होने के बावजूद स्वार्म व्यवहार संगठित और कुशल रहता है।

फॉर्मेशन नियंत्रण

क्लस्टर के सदस्य अपने क्लस्टर के भीतरी फॉर्मेशन को प्रबंधित करते हैं सिमुलेशन के समयक्षेत्रों के सटीक बटवारे के कारण क्लस्टर के फॉर्मेशन में बहुत बड़े बदलाव नहीं किये गये।

संसाधन आवंटन

क्वीन ड्रोन बैटरी उपयोग और डेटा प्रसारण स्थान की अद्त व्यवस्था करते हैं। संसाधन आवंटन रणनीतियाँ ऊर्जा उपयोग को अनुकूलित करने और मिशन अवधि को बढ़ाने में सफल होती हैं।

अनुकूलन मूल्यांकन:

क्लस्टर स्वार्म सफलतापूर्वक अपने अपने क्षेत्र के अनुसार प्रारंभिक फॉर्मेशन बनाने तथा उसे मिशन के दौरान पूरे समय तक समायोजित रखने में सफल रहे। सभी एजेंट ड्रोन्स अपने आस पास के अवरोधों

(ऑब्जेक्ट्स) को बिना अपने गठन की मूलभूत संरचना को तोड़े हुए टालने में भी सफल रहे ।

निष्कर्ष

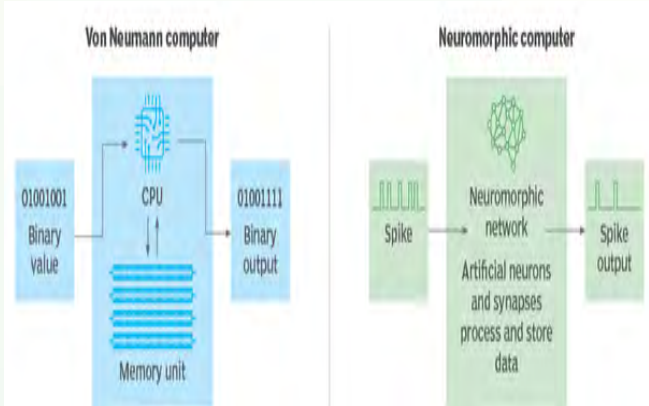
यह वैचारिक ढांचा, सिमुलेशन में अपने दिए गये कार्य को आदर्श जानकारी के साथ पूरा करने में सफल रहा, इस सिमुलेशन का मुख्य लक्ष्य यह देखना था की क्लस्टर स्वार्म्स किस तरह अपने स्वार्म के गुणों के साथ क्वीन ड्रोन के साथ कनेक्शन स्थापित कर पाते हैं तथा किस तरह से सेन्सर्स एल्गोरिदम, टोकन एल्गोरिदम , नेविगेशन एल्गोरिदम सेल्फ फॉर्मेशन एल्गोरिदम के साथ कार्य कर पाते हैं।

ReRAM पर आधारित न्यूरोमॉर्फिक कंप्यूटिंग

श्री राम सिंह बैरवा, वैज्ञानिक "सी"

परिचय (Introduction):

आजकल, मशीन लर्निंग और IoT जैसी तकनीकों ने औद्योगिक स्वचालन (industrial automation) से लेकर बिजनेस मॉडल भविष्यवाणी तक कई क्षेत्रों को संभव बना दिया है। ड्रोन, ऑटोनोमस कारें, स्मार्ट हेल्थकेयर, स्मार्ट सिटी और कई अन्य प्रौद्योगिकियां अधिक से अधिक डेटा उत्पन्न कर रही है और क्लाउड से जुड़े उपकरणों की संख्या भी बढ़ रही हैं। बढ़ते उपकरणों के परिणामस्वरूप डेटा एवं प्रोसेसिंग में वृद्धि हो रही है जिससे वर्तमान भंडारण उपकरणों और प्रोसेसिंग उपकरणों के लिए चुनौतियाँ बढ़ रही हैं। पारंपरिक कंप्यूटरों में डेटा प्रोसेसिंग (CPU) और मेमोरी के बीच की फिजीकल दूरी के परिणामस्वरूप पॉवर की खपत एवं डेटा गणना मे विलंबता में वृद्धि हुई है| इन चुनौतियो को दूर करने के लिए वॉन न्यूमैन (Von Neumann) कंप्यूटिंग आर्किटेक्चर के बजाय न्यूरोमॉर्फिक (Neuromorphic) कंप्यूटिंग आर्किटेक्चर एक लोकप्रिय आर्किटेक्चर बन गई है। न्यूरोमॉर्फिक आर्किटेक्चर के कई महत्वपूर्ण लाभ हैं, जैसे वास्तविक समय (Real-time) प्रदर्शन, समानांतरवाद, वॉन न्यूमैन बॉटलनेक, स्केलेबिलिटी, कम पॉवर, फूटप्रिंट, दोष सहनशीलता, तेज़ और ऑनलाइन लर्निंग। न्यूरोमॉर्फिक कंप्यूटिंग मानव मस्तिष्क और तंत्रिका तंत्र से प्रेरित है। न्यूरोमॉर्फिक कंप्यूटिंग आर्किटेक्चर की इन विशेषताओं के कारण मशीन लर्निंग एल्गोरिदम को इम्प्लिमेंट करने का एक उपयुक्त विकल्प प्रदान करता है |

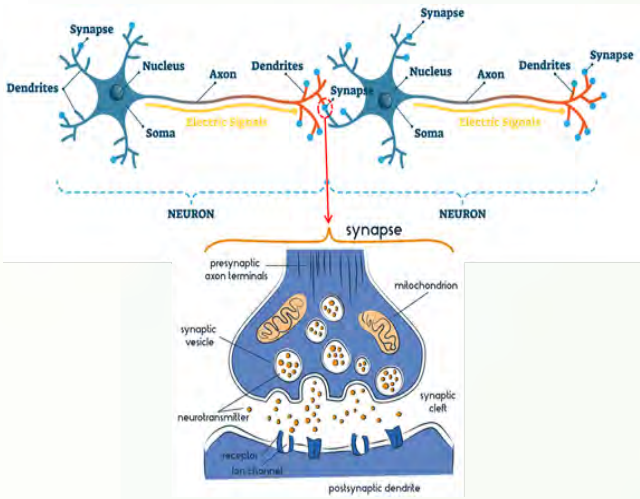


चित्र: 1- वॉन न्यूमैन एवं न्यूरोमॉर्फिक आर्किटेक्चर

तंत्रिका विज्ञान अवधारणाएँ (Neuroscience Concepts):

न्यूरॉन तंत्रिका तंत्र की मूलभूत इकाई हैं जो शरीर के विभिन्न भागों से सिग्नल प्राप्त करता हैं तथा संचारित करता हैं। न्यूरॉन के तीन भाग होते हैं - डेंड्राइट्स, सेल बॉडी और एक्सॉन। न्यूरॉन सिनैप्स के माध्यम से अन्य कोशिकाओं के साथ संचार करता हैं। - एक विशेष कनेक्शन जो प्रीसिनेप्टिक न्यूरॉन से सिनैप्टिक गैप के माध्यम से पोस्ट सिनैप्टिक न्यूरॉन तक सिग्नल पहुचता है। रासायनिक न्यूरोट्रांसमीटर, प्रीसिनेप्टिक न्यूरॉन से पोस्ट सिनैप्टिक न्यूरॉन तक सिग्नल पहुचाने का काम करते हैं।

एक परिपक्व मानव मस्तिष्क में लगभग 100 अरब न्यूरॉन होते हैं और एक न्यूरॉन में लगभग 103-104 सिनैप्स होते हैं। समग्र बुद्धिमत्ता न्यूरॉन की संख्या और अन्य न्यूरॉन्स के साथ कनेक्टिविटी पर निर्भर करती है।



चित्र: 2- न्यूरॉन और सिनैप्स की संरचना

न्यूरोमोर्फिक कंप्यूटिंग (Neuromorphic Computing):

मानव मस्तिष्क न्यूरोमॉर्फिक कंप्यूटिंग का सबसे अच्छा उदाहरण है जिसमें लगभग 100 बिलियन न्यूरॉन होते हैं और केवल 20W बिजली की खपत होती है। मस्तिष्क में मेमोरी और प्रोसेसर इस तरह व्यवस्थित होते हैं कि सीखने की प्रक्रिया के आधार पर घटकों की अलग-

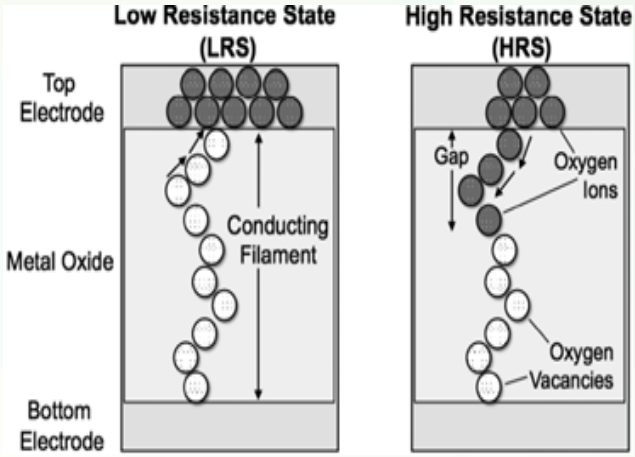
अलग भूमिकाएँ हो सकती हैं। इसके अलावा, मस्तिष्क एक लचीली प्रणाली है जो जटिल वातावरण, स्व-प्रोग्रामिंग और जटिल प्रसंस्करण में सक्षम है।

ReRAM तकनीकी का उपयोग करके न्यूरो-प्रेरित कंप्यूटिंग (Neuro-Inspired computing using ReRAM Technology):

जैविक तंत्रिका नेटवर्क से पता चलता है कि न्यूरो-प्रेरित कंप्यूटिंग का मूल कार्य हार्डवेयर प्रौद्योगिकी का उपयोग करके मौलिक सिनैप्स, न्यूरॉन्स और उनके सिनैप्टिक व्यवहार को दोहराना है। न्यूरोमॉर्फिक प्रणाली में सबसे महत्वपूर्ण घटकों में से एक इलेक्ट्रॉनिक सिनैप्स को उच्च एकीकरण घनत्व (high integration density) और कम ऊर्जा खपत की आवश्यकता है। नॉन-वोलेटाइल मेमोरी (NVM) के क्रॉसबार ऐरे बड़े पैमाने पर समानांतर और अत्यधिक एनर्जी एफिसिएन्ट, न्यूरोमॉर्फिक कंप्यूटिंग सिस्टम को सक्षम बना सकते हैं। NVM तत्वों के लिए मुख्य निरंतर (एनालॉग) चालन ट्यूनिंग क्षमता और स्वीकार्य नॉइज लेवल के साथ स्विचिंग समरूपता आवश्यक हैं।

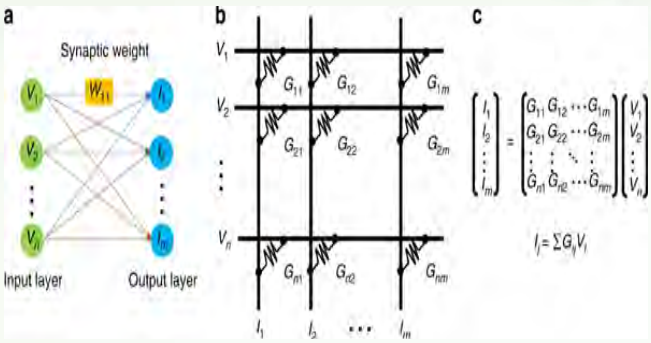
मेटल ऑक्साइड आधारित प्रतिरोधक स्विचिंग या प्रतिरोधक रैंडम एक्सेस मेमोरी डिवाइस (ReRAM) अपनी मल्टी-लेवल और नॉन-वोलेटाइल डेटा भंडारण क्षमता, कम ऊर्जा खपत और सरल डिवाइस संरचना के कारण इलेक्ट्रॉनिक्स सिनैप्स के लिए सबसे उपयुक्त है।

ReRAM डिवाइस एक मेटल-इन्सुलेटर-मेटल (MIM) कॉन्फ़िगरेशन है जो हिस्टेरेटिक प्रतिरोधी स्विचिंग व्यवहार प्रदर्शित करती है। ReRAM के संचालन का सिद्धांत जहाँ मेटल-ऑक्साइड परत दो इलेक्ट्रोडों के बीच सैंडविच होती है। यह संरचना कम-प्रतिरोध स्थिति (LRS) और उच्च-प्रतिरोध स्थिति (HRS) के बीच एक प्रतिरोधी स्विचिंग घटना प्रदर्शित करती है, जो कि ऑक्सीजन माईग्रेसन प्रक्रियाओं के कारण होती है। अलग-अलग मानों को दर्शाने के लिए डिवाइस पर अलग-अलग प्रतिरोध मान लिखे जा सकते हैं। LRS प्रक्रिया के दौरान धातु इलेक्ट्रोड-ऑक्साइड इंटरफेश पर जब एक सेट वोल्टेज लागू किया जाता है, तो ऑक्सीजन के बहाव के कारण प्रवाहकीय फिलामेंट्स दिखाई देता हैं। HRS प्रक्रिया के दौरान जब एक रीसेट वोल्टेज लागू किया जाता है, तो ऑक्सीजन आयन वापस चले जाते हैं और आंशिक रूप से रिक्तियों को भर देते हैं, जिससे प्रवाहकीय फिलामेंट में एक अंतर पैदा हो जाता है और परिणामस्वरूप प्रवाहकीय फिलामेंट्स नहीं दिखाई देता हैं। जैसा कि चित्र 3 में दिखाया गया है।



चित्र: 3- ReRAM डिवाइस की निम्न और उच्च-प्रतिरोध स्थिति

जैसा कि चित्र 4 में दिखाया गया है, ReRAM और फेस-चेन्ज मेमोरी (PCM) का परिवर्तनीय कंडक्टेन्स करना संभव है। ReRAM के परिवर्तनीय कंडक्टेन्स का उपयोग सिनैप्टिक भार को रीपर्जेंट करने और वेक्टर-मैट्रिक्स गुणन करने के लिए किया जा सकता है। वेक्टर-मैट्रिक्स गुणन करने के लिए बुनियादी विद्त सिद्धांतों जैसे ओम और किरचॉफ के नियमो का उपयोग किया जाता है, जो बड़े पैमाने पर स्थानीय और समानांतर गणना को सक्षम बनाते हैं। ReRAM के कंडक्टेन्स परिवर्तन को द्विदिशात्मक बनाकर, बैक-प्रॉपैगेशन एल्गोरिदम को लागू किया जा सकता है। ReRAM के इस तरह के क्रॉसबार ऐरे से डीप न्यूरल नेटवर्क (DNN) प्रशिक्षण मे एसेलेरेसन, पॉवर और क्षेत्रफल में कमी प्राप्त की जा सकती है। अनुसंधान का एक अन्य सक्रिय क्षेत्र स्पाइकिंग न्यूरल नेटवर्क (SNN) है जो अधिक जैविक रूप से न्यूरल नेटवर्क मॉडल बनाने की आवश्यकता से प्रेरित है। कई न्यूरोमॉर्फिक कंप्यूटिंग प्लेटफ़ॉर्म विकसित किए जा रहे हैं जो स्पाइक-आधारित गणना का अनुकरण करने के लिए अनुकूलित हैं। इन SNN को आम तौर पर कुछ लोकल नियमों का उपयोग करके प्रशिक्षित किया जाता है, जैसे कि स्पाइक-टाइमिंग-डिपेन्डेन्ट प्लास्टिसिटी। ReRAM डिवाइस को SNN के मूल एलेमेन्ट, सिनैप्टिक और न्यूरोनल को बनाने में प्रयोग मे लाया जा रहा है।



चित्र: 4- NVM (ReRAM) पर आधारित न्यूरोमॉर्फिक कंप्यूटिंग प्रणाली। a एक इनपुट परत को आउटपुट परत से जोड़ने वाले सिनैप्टिक वेट (W) के साथ एक-परत न्यूरल नेटवर्क का एक योजनाबद्ध चित्रण। b एक सिनैप्टिक भार को प्रत्येक NVM के संचालन मूल्य द्वारा दर्शाया जाता है

क्रॉसबार ऐरे में ReRAM उपकरणों के कुछ नॉन-आईडल प्रभाव हैं। ReRAM के नॉन-आईडल प्रभाव स्थैतिक दोष (static defects) और परिवर्तनशीलता के साथ-साथ गतिशील परिवर्तनशीलता (dynamic variability) भी हैं। स्टक-एट-फौल्ट (Stuck-at-Faults), फेबरिकेसन प्रोसेस में कमियाँ और निर्माण प्रक्रिया के खराब नियंत्रण के कारण होता है जिससे सेट या रीसेट संचालन की परवाह किए बिना, ReRAM डिवाइस का प्रतिरोध मान HRS या LRS पर अटक जाता है। रैंडम टेलीग्राफ नॉइज (Random Telegraph Noise), जाली दोषों की उपस्थिति, चार्ज का रेंडम ट्रेप तथा चार्ज के रीलीज की उपस्थिति के कारण होता है, ReRAM डिवाइस दो स्थिर स्थितियों (LRS & HRS) के बीच यादृच्छिक रूप से उतार-चढ़ाव करता है। राईट परिवर्तनशीलता (Write Variability) सेट और रीसेट स्थितियों के प्रतिरोध मूल्यों के कारण है।

न्यूरोमॉर्फिक चिप्स पर वर्तमान में IBM , Intel आदि जैसे कई कंप्यूटर दिग्गजों द्वारा बड़े पैमाने पर शोध किया जा रहा है। NVM और कृत्रिम सिनैप्स के क्षेत्र में अनुसंधान ने न्यूरोमॉर्फिक चिप्स में क्रांति ला दी है।

निष्कर्ष (Conclusion):

पूरी दुनिया आर्टिफिशियल इंटेलिजेंस की ओर तेजी से बढ़ रही है। 2030 के अंत तक, क्लाउड से जुड़े उपकरणों की संख्या हमारे पास अब की तुलना में तेजी से बढ़ जाएगी। क्लाउड पर बढ़ते उपकरणों का अर्थ है डेटा ट्रैफ़िक में वृद्धि और बड़ी हार्डवेयर वास्तुकला की आवश्यकता। दुर्भाग्य से वर्तमान उपकरणों के लिए भी, डेटा ट्रैफ़िक अधिक है और काफी मात्रा में ऊर्जा और संसाधनों का उपयोग किया जा रहा है। न्यूरोमॉर्फिक कंप्यूटिंग को इन समस्याओं के समाधान के रूप में देखा जाता है क्योंकि यह बड़ी मात्रा में डेटा को संभालने में सक्षम है और इसके लिए ऊर्जा की खपत को काफी कम कर देता है। आर्टिफिशियल सिनैप्स अभूतपूर्व तकनीक है जो न्यूरोमॉर्फिक कंप्यूटिंग को वास्तविकता में बदल देती है। अभी भी कृत्रिम सिनेप्स के लाभ को पूरी तरह से समझने और उपयोग करने के लिए शोध जारी है। ReRAM उन्नति के उस स्तर का सबसे अच्छा उदाहरण और प्रमाण है जो हमने हाल ही में हासिल किया है और हमें कृत्रिम बुद्धिमत्ता की दुनिया में आगे ले गया है। भौतिक और तकनीकी सीमाओं और चुनौतियों के बावजूद, न्यूरोमॉर्फिक कंप्यूटिंग लगातार महत्वपूर्ण दर से बढ़ रही है और निकट भविष्य में कंप्यूटिंग के दृष्टिकोण में अच्छे बदलाव की उम्मीद है।

संदर्भ (Reference):

1. R Vishwa, "Current Research and Future Prospects of Neuromorphic Computing in Artificial Intelligence" IOP Conf. 2020.
2. M. K. LEE, Y. CUI, T. SOMU, T. LUO, J. ZHOU, W. TANG, W. WONG, R. S. GOH, "A System-Level Simulator for RRAM-Based Neuromorphic Computing Chips"
3. ZHEQI, AMIR M. ABDULGHANI ADNAN, HADI HEIDARI MUHAMMAD ALI IMRAN AND QAMMER H. ABBASI "An Overview of Neuromorphic Computing for Artificial Intelligence Enabled Hardware-Based Hopfield Neural Network" 2020.
4. Gaithersburg, "Neuromorphic computing: From Materials to System Architecture" 2015.
5. S. Park, H. Kim, M. Choo, J. Noh, A. Sheri, S. Jung, K. Seo, J. Park, S. Kim, W. Lee & J. Shin, "RAM-based synapse for neuromorphic system with pattern recognition function" International Electron Devices Meeting 2012.
6. J.F. Kang, B. Gao; P. Huang, L.F. Liu, X.Y. Liu, H.Y. Yu, S. Yu & H.-S. Philip Wong, "RRAM based synaptic devices for neuromorphic visual systems" IEEE International Conference on Digital Signal Processing (DSP) 2015.
7. N. Gong, T. Idé, S. Kim I. Boybat, A. Sebastian, V. Narayanan & T. Ando "Signal and noise extraction from analog memory elements for neuromorphic computing" Nature Cmmunications 2018
8. https://www.techtarget.com/searchenterpriseai/definition/neuromorphic-computing
9. https://www.healthline.com/health/neurons#anatomy
10. https://www.simplypsychology.org/synapse.html

ए०आई० आधारित प्रणालियों के लिए IV&V प्रक्रिया पर आलोचनात्मक विवेचन

श्री सौरभ मांडल, वैज्ञानिक-एफ

प्रस्तावना

हाल के दिनों में, विभिन्न क्षेत्रों और भौगोलिक क्षेत्रों के व्यवसाय विभिन्न व्यावसायिक प्रक्रियाओं और अनुप्रयोगों के प्रदर्शन, दक्षता और प्रबंधन को बढ़ाने में एआई की बहुमुखी प्रतिभा और महत्व को खोज रहे हैं। इसके अलावा, निवेश पर बेहतर रिटर्न के वादे पर सवार होकर, एआई महत्वपूर्ण प्रणालियों में भी अपना अनुप्रयोग ढूंढ रहा है। जैसे-जैसे प्रौद्योगिकी का विकास जारी है, एआई इन महत्वपूर्ण प्रणालियों की दक्षता और विश्वसनीयता सुनिश्चित करने में और भी महत्वपूर्ण भूमिका निभाएगा। इसलिए, इन एआई आधारित प्रणालियों को वास्तविक दुनिया यानी क्षेत्र के वातावरण में तैनात करने से पहले स्वतंत्र परीक्षण और सत्यापन (आईवी एंड वी) के अधीन करना अनिवार्य हो जाता है। पिछले कुछ वर्षों में, IV&V के लिए उद्योग की सर्वोत्तम पद्धतियां पारंपरिक सॉफ्टवेयर प्रणालियों के लिए अच्छी तरह से स्थापित की गई हैं। हालाँकि, आर्टिफिशियल इंटेलिजेंस (एआई) के उदय के साथ, एआई-आधारित प्रणालियों द्वारा उत्पन्न अद्वितीय चुनौतियों का समाधान करने के लिए इन प्रथाओं को अनुकूलित और विस्तारित करने की आवश्यकता है। यह लेख इसी विषय पर एक आलोचनात्मक विवेचना का प्रयास करता है, जिसके माध्यम से हम ना सिर्फ वर्तमान में प्रयुक्त IV&V पद्धतियों के बारे में जानेंगे, अपितु यह भी देखेंगे कि ए०आई० आधारित प्रणालियों के लिए इन पद्धतियों में क्या परिवर्तन एवं अनुकूलन अपेक्षित हैं। अंततः मौजूदा IV&V प्रक्रियाओं में कुछ बदलावों का सुझाव दिया गया है, ताकि संशोधित प्रक्रियाओं को AI सिस्टम की उभरती दुनिया में अपने इच्छित लक्ष्यों को प्राप्त किया जा सके।

परिचय

स्वतंत्र परीक्षण और सत्यापन (IV&V) सॉफ्टवेयर विकास जीवनचक्र (SDLC) में एक महत्वपूर्ण चरण है, जो यह सुनिश्चित करता है कि सॉफ्टवेयर सिस्टम अपनी निर्दिष्ट आवश्यकताओं को पूरा करें और उद्देश्य के अनुसार कार्य करें। पारंपरिक सॉफ्टवेयर सिस्टम के लिए स्थापित IV&V प्रथाओं में आम तौर पर आवश्यकता विश्लेषण, डिज़ाइन सत्यापन, परीक्षण और परिनियोजन सत्यापन को शामिल करने वाला एक व्यवस्थित दृष्टिकोण शामिल होता है। कठोर परीक्षण पद्धतियाँ, कोडिंग मानकों का पालन और संपूर्ण दस्तावेज़ीकरण सॉफ़्टवेयर गुणवत्ता सुनिश्चित करने के स्तंभ रहे हैं। IV&V के लिए आईएसओ (ISO) और IEEE द्वारा अनुशंसित मानक बहुत परिपक्वता के साथ स्थापित हैं। इनका बहुतायत पालन भी किया जाता है और इनकी स्वीकार्यता भी विस्तृत हैं। इसके अलावा, पारंपरिक सॉफ्टवेयर प्रणालियों के लिए कुछ उद्योग-विशिष्ट प्रथाएं व मानक हैं जैसे कि डीआरडीओ प्रयोगशालाओं द्वारा विकसित अनुसंधान एवं विकास परियोजनाओं और उत्पादों के लिए सॉफ्टवेयर विकास के लिए डीआरडीओ द्वारा निर्धारित एक मानक – "डीएसएसडी" ।

एआई-आधारित सिस्टम पर IV&V प्रक्रियाओं की प्रयोज्यता

जैसे-जैसे एआई-आधारित प्रणालियाँ तेजी से प्रचलित होती जा रही हैं, मजबूत IV&V प्रक्रियाओं की आवश्यकता अधिक स्पष्ट होती जा रही है। IV&V के मूलभूत सिद्धांत, जैसे आवश्यकताओं का विश्लेषण और परीक्षण, अभी भी लागू हैं। हालाँकि, एआई सिस्टम की अनूठी विशेषताओं, जैसे कि जटिल एल्गोरिदम और बड़े डेटासेट पर उनकी निर्भरता, के लिए एक सूक्ष्म दृष्टिकोण की आवश्यकता होती है।

एआई के संदर्भ में, IV&V पारंपरिक सीमाओं से परे फैला हुआ है, जिसमें न केवल पारंपरिक सॉफ्टवेयर घटक बल्कि अंतर्निहित मशीन लर्निंग मॉडल भी शामिल हैं। समय के साथ एआई मॉडल की अनुकूलनशीलता के लिए निरंतर सत्यापन की आवश्यकता होती है, जिससे पारंपरिक सत्यापन, जो कमोवेश एक ही बार किया जाता है, अपर्याप्त हो जाता है।

एआई-आधारित प्रणालियों में IV&V प्रक्रियाओं को लागू करने में चुनौतियाँ

एआई-आधारित प्रणालियों में IV&V प्रक्रियाओं को लागू करने में विविध चुनौतियों और विचारों को स्पष्ट

करने के लिए, कुछ उदाहरणों और वास्तविक दुनिया के मामलों पर यहां चर्चा की गई है। कोई भी इन मामलों से अंतर्दृष्टि प्राप्त करके अपनी स्वयं की IV&V रणनीतियाँ बना सकता है, जिससे यह सुनिश्चित हो सके कि AI अनुप्रयोग गुणवत्ता, नैतिकता और विश्वसनीयता के उच्च मानकों को पूरा करते हैं। यह ध्यान में रखना चाहिए कि एआई का क्षेत्र गतिशील है, और सूचित निर्णय लेने के लिए नवीनतम केस स्टडीज के साथ अपडेट रहना आवश्यक है।

केस 1: 2018 में, अमेज़ॅन को जांच का सामना करना पड़ा जब यह बताया गया कि उनके एआई-आधारित हायरिंग टूल ने लिंग पूर्वाग्रह प्रदर्शित किया। टूल को 10 साल की अवधि में कंपनी को सौंपे गए बायोडाटा पर प्रशिक्षित किया गया था, जो मुख्य रूप से पुरुष आवेदकों से आया था। यह मामला IV&V के दौरान कठोर डेटा गुणवत्ता मूल्यांकन और पूर्वाग्रह का पता लगाने के महत्व पर प्रकाश डालता है। एआई निर्णय लेने में पक्षपाती परिणामों को रोकने के लिए प्रशिक्षण डेटा में प्रतिनिधित्व सुनिश्चित करना महत्वपूर्ण है।

अंतर्दृष्टि: डेटा गुणवत्ता और पूर्वाग्रह शमन सुनिश्चित करने के लिए डेटा-केंद्रित सत्यापन आवश्यक है

केस 2: शोधकर्ताओं ने प्रतिकूल हमलों का उपयोग करके चेहरे की पहचान प्रणालियों में कमजोरियों का प्रदर्शन किया। इनपुट छवियों में सूक्ष्म परिवर्तन करके, वे चेहरों को गलत वर्गीकृत करने के लिए एआई मॉडल को गुमराह कर सकते हैं। यह IV&V के दौरान प्रतिकूल परिदृश्यों के विरुद्ध मजबूत एल्गोरिथम सत्यापन और परीक्षण की आवश्यकता को रेखांकित करता है। चेहरे की पहचान प्रणालियों पर निर्भर संस्थानों और कंपनियों को ऐसे हमलों का मुकाबला करने के लिए उपाय लागू करने की आवश्यकता है।

अंतर्दृष्टि: प्रतिकूल हमलों से सुरक्षा के लिए एल्गोरिथम सत्यापन की आवश्यकता है

केस 3: एक सैन्य एआई प्रोजेक्ट, प्रोजेक्ट मावेन में Google की भागीदारी को कर्मचारियों और बाहरी हितधारकों से विरोध का सामना करना पड़ा। सैन्य अनुप्रयोगों में एआई के उपयोग के संबंध में नैतिक चिंताओं ने Google को एआई के लिए नैतिक सिद्धांत स्थापित करने के लिए प्रेरित किया। यह मामला IV&V के दौरान नैतिक प्रभाव आकलन के महत्व पर जोर देता है, खासकर उन परिदृश्यों में जहां एआई अनुप्रयोगों में सैन्य उपयोग के मामले या सामाजिक निहितार्थ हो सकते हैं।

अंतर्दृष्टि: प्रभाव आकलन पर आधारित नैतिक और नियामक अनुपालन

केस 4: डायग्नोस्टिक्स के लिए एआई को एकीकृत करने वाली हेल्थकेयर प्रणालियों को मौजूदा इलेक्ट्रॉनिक हेल्थ रिकॉर्ड (ईएचआर) सिस्टम के साथ अंतरसंचालनीयता चुनौतियों का सामना करना पड़ सकता है। इस संदर्भ में IV&V को स्वास्थ्य पेशेवरों के कार्यप्रवाह में व्यवधानों से बचने के लिए निर्बाध एकीकरण सुनिश्चित करना चाहिए। हेल्थकेयर एआई कार्यान्वयन से जुड़े केस अध्ययन व्यापक अंतरसंचालनीयता परीक्षण की आवश्यकता पर प्रकाश डालते हैं।

अंतर्दृष्टि: मौजूदा प्रणालियों के साथ अंतरसंचालनीयता और अनुकूलनशीलता सुनिश्चित करने के लिए परीक्षण

केस 5: टेस्ला के ऑटोपायलट सिस्टम को निर्णय लेने में पारदर्शिता की कमी के लिए आलोचना का सामना करना पड़ा। सिस्टम की निर्णय लेने की प्रक्रिया, मालिकाना होने के कारण, उपयोगकर्ता की समझ और सुरक्षा के बारे में चिंताएँ बढ़ाती है। IV&V प्रक्रियाओं को पारदर्शिता और व्याख्यात्मकता को संबोधित करने की आवश्यकता है, यह सुनिश्चित करते हुए कि उपयोगकर्ता और हितधारक एआई निर्णयों के पीछे के तर्क को समझ सकें।

अंतर्दृष्टि: तर्क को समझने और जवाबदेही तय करने के लिए पारदर्शिता और व्याख्या

केस 6: चैटबॉट और वर्चुअल असिस्टेंट, जैसे कि फेसबुक और गूगल जैसी कंपनियों द्वारा तैनात किए गए, उपयोगकर्ता की बातचीत के आधार पर लगातार विकसित होते रहते हैं। इस संदर्भ में IV&V में उपयोगकर्ता प्रतिक्रिया की निगरानी करना, सुधार के क्षेत्रों की पहचान करना और एआई की संवादात्मक क्षमताओं को बढ़ाने के लिए अपडेट तैनात करना शामिल है। इन अनुकूली एआई प्रणालियों की प्रभावशीलता को बनाए रखने के लिए निरंतर सत्यापन महत्वपूर्ण है।

अंतर्दृष्टि: प्रभावशीलता बनाए रखने के लिए निरंतर सुधार और फीडबैक एकीकरण

एआई-आधारित सिस्टम के लिए IV&V प्रक्रियाओं में विशिष्ट परिवर्तन

लगातार विकसित हो रही एआई आधारित प्रणालियों द्वारा पेश की गई नई चुनौतियों का समाधान करने के

लिए मौजूदा IV&V प्रक्रियाओं को संवर्धित करने की आवश्यकता है। मौजूदा प्रथाओं में कुछ प्रस्तावित संशोधन नीचे सूचीबद्ध हैं:

1. डेटा-केंद्रित सत्यापन: एआई मॉडल प्रशिक्षण और निर्णय लेने के लिए डेटा पर बहुत अधिक निर्भर करते हैं। एआई के लिए IV&V में प्रशिक्षण डेटा गुणवत्ता, प्रासंगिकता और संभावित पूर्वाग्रहों की सावधानीपूर्वक जांच शामिल होनी चाहिए। इसके लिए डेटा स्रोतों की गहन समझ और उनकी प्रतिनिधित्वशीलता के निरंतर मूल्यांकन की आवश्यकता होती है।

2. एल्गोरिथम सत्यापन: पारंपरिक सॉफ्टवेयर सिस्टम नियतात्मक होते हैं, जबकि एआई सिस्टम संभाव्य और गैर-नियतात्मक होते हैं। एआई एल्गोरिदम को मान्य करने में उनकी सटीकता, परिशुद्धता और रिकॉल का आकलन करना शामिल है। इसके अतिरिक्त, प्रतिकूल हमलों और अप्रत्याशित इनपुट के खिलाफ मॉडल की मजबूती का परीक्षण करना महत्वपूर्ण है।

3. नैतिक और नियामक अनुपालन: एआई सिस्टम नैतिक विचारों और नियामक चुनौतियों को बढ़ाता है जो पारंपरिक सॉफ्टवेयर से परे हैं। एआई के लिए IV&V को नैतिक दिशानिर्देशों और गोपनीयता नियमों का अनुपालन सुनिश्चित करना चाहिए। इसमें एआई निर्णय लेने में पूर्वाग्रहों की पहचान करने और उन्हें कम करने के लिए नैतिक प्रभाव आकलन करना शामिल है।

4. इंटरऑपरेबिलिटी और अनुकूलनशीलता: एआई के लिए IV&V प्रक्रियाओं को अन्य सॉफ्टवेयर घटकों के साथ एआई मॉड्यूल की इंटरऑपरेबिलिटी को संबोधित करना चाहिए। इसके अलावा, समय के साथ एआई मॉडल की अनुकूलनशीलता के लिए निरंतर निगरानी और सत्यापन की आवश्यकता होती है ताकि यह सुनिश्चित किया जा सके कि वे बदलते परिवेश में सर्वोत्तम प्रदर्शन करें।

5. पारदर्शिता और व्याख्यात्मकता: पारंपरिक सॉफ़्टवेयर के विपरीत जहां तर्क स्पष्ट रूप से कोडित होता है, एआई मॉडल, विशेष रूप से गहन शिक्षण मॉडल, को "ब्लैक बॉक्स" के रूप में माना जा सकता है। एआई निर्णय लेने की प्रक्रियाओं की पारदर्शिता और व्याख्या सुनिश्चित करना एआई के लिए IV&V में एक अनूठी चुनौती बन गई है।

6. निरंतर सुधार और फीडबैक एकीकरण: एआई विकास की पुनरावृत्तीय प्रकृति के लिए निरंतर सत्यापन और अद्यतन की आवश्यकता होती है। इसलिए, यह सुनिश्चित करने के लिए कि एआई सिस्टम समय के साथ प्रभावी और प्रासंगिक बना रहे, IV&V प्रक्रियाओं को चल रही निगरानी, फीडबैक एकीकरण और अनुकूलन का समर्थन करना चाहिए।

एआई-आधारित सिस्टम में IV&V के लिए चरण-दर-चरण प्रक्रिया

एआई-आधारित सिस्टम में स्वतंत्र परीक्षण और सत्यापन (IV&V) के लिए चरण-दर-चरण प्रक्रिया में यह सुनिश्चित करना शामिल है कि सिस्टम अपनी निर्दिष्ट आवश्यकताओं को पूरा करता है, अपेक्षा के अनुरूप व्यवहार करता है और दोषों से मुक्त है। इसके अतिरिक्त, ऐसे संवर्द्धन भी हैं जिनकी चर्चा पिछले अनुभागों में की गई है। इन सबको एक साथ रखते हुए, यहां AI-आधारित सॉफ़्टवेयर और सिस्टम में IV&V के लिए 12-चरणीय प्रक्रिया दी गई है:

1. आवश्यकताएँ विश्लेषण:

क) एआई प्रणाली के व्यावसायिक उद्देश्यों और कार्यात्मक आवश्यकताओं को समझें।

ख) एआई कार्यक्षमता, प्रदर्शन और विश्वसनीयता से संबंधित विशिष्ट आवश्यकताओं को पहचानें और उनका दस्तावेजीकरण करें।

2. डेटा संग्रह और विश्लेषण:

क) प्रशिक्षण डेटा की गुणवत्ता और प्रासंगिकता का आकलन करें।

ख) सत्यापित करें कि प्रशिक्षण डेटासेट प्रतिनिधि और निष्पक्ष है।

ग) यह सुनिश्चित करने के लिए डेटा की विविधता और वितरण का विश्लेषण करें कि यह सभी प्रासंगिक परिदृश्यों को कवर करता है।

3. मॉडल विकास:

क) एआई मॉडल आर्किटेक्चर और डिज़ाइन की समीक्षा करें।

ख) सत्यापित करें कि मॉडल सर्वोत्तम प्रथाओं और नैतिक दिशानिर्देशों का पालन करता है।

ग) मॉडल की पारदर्शिता और व्याख्यात्मकता का आकलन करें।

4. एल्गोरिथम सत्यापन:

क) सटीकता, परिशुद्धता, रिकॉल और अन्य प्रासंगिक मेट्रिक्स के लिए एआई एल्गोरिदम का मूल्यांकन करें।

ख) किनारे के मामलों सहित विविध डेटासेट के साथ मॉडल का परीक्षण करें।

ग) सत्यापित करें कि मॉडल समय के साथ और विभिन्न परिवेशों में लगातार प्रदर्शन करता है।

5. परीक्षण और मूल्यांकन:

क) एआई कार्यक्षमता के विभिन्न पहलुओं को शामिल करते हुए व्यापक परीक्षण मामले विकसित करें।

ख) एआई सिस्टम के लिए यूनिट परीक्षण, एकीकरण परीक्षण और सिस्टम परीक्षण करें।

ग) सिस्टम के प्रदर्शन, स्केलेबिलिटी और प्रतिक्रिया का मूल्यांकन करें।

6. नैतिक और नियामक अनुपालन:

क) सुनिश्चित करें कि एआई प्रणाली नैतिक दिशानिर्देशों और कानूनी नियमों का अनुपालन करती है।

ख) सत्यापित करें कि सिस्टम गोपनीयता और सुरक्षा आवश्यकताओं का पालन करता है।

ग) संभावित पूर्वाग्रहों की पहचान करने और उन्हें कम करने के लिए नैतिक प्रभाव मूल्यांकन का संचालन करें।

7. अंतरसंचालनीयता परीक्षण:

क) अन्य सॉफ्टवेयर घटकों के साथ एआई सिस्टम के एकीकरण का परीक्षण करें।

ख) सत्यापित करें कि एआई सिस्टम बाहरी सिस्टम और एपीआई के साथ निर्बाध रूप से बातचीत कर सकता है।

8. मजबूती और लचीलापन परीक्षण:

क) शोर या अधूरे डेटा को संभालने के लिए एआई सिस्टम की मजबूती का आकलन करें।

ख) प्रतिकूल हमलों या अप्रत्याशित इनपुट के प्रति सिस्टम की लचीलापन का परीक्षण करें।

9. दस्तावेज़ीकरण समीक्षा:

क) मॉडल दस्तावेज़ीकरण, उपयोगकर्ता मैनुअल और तकनीकी विशिष्टताओं सहित सभी दस्तावेज़ों की करें।

ख) सुनिश्चित करें कि दस्तावेज़ीकरण कार्यान्वित एआई प्रणाली को सटीक रूप से दर्शाता है।

10. परिनियोजन सत्यापन:

क) सत्यापित करें कि परिनियोजन प्रक्रिया अच्छी तरह से प्रलेखित और त्रुटि रहित है।

ख) यह सुनिश्चित करने के लिए कि सिस्टम अपेक्षा के अनुरूप काम करता है, उत्पादन परिवेश में परीक्षण करें।

11. निगरानी और रखरखाव:

क) वास्तविक दुनिया के परिदृश्यों में एआई प्रणाली के प्रदर्शन को ट्रैक करने के लिए निगरानी उपकरण लागू करें।

ख) निरंतर सुधार, अद्यतन और उभरते मुद्दों के समाधान के लिए एक रखरखाव योजना स्थापित करें।

12. फीडबैक लूप एकीकरण:

क) उपयोगकर्ताओं और हितधारकों से फीडबैक एकत्र करने के लिए तंत्र स्थापित करें।

ख) एआई मॉडल को बेहतर बनाने और उभरती आवश्यकताओं को पूरा करने के लिए सिस्टम को अपडेट करने के लिए फीडबैक का उपयोग करें।

इस व्यापक 12-चरणीय प्रक्रिया का पालन करके, कोई भी स्वतंत्र परीक्षण और सत्यापन के माध्यम से एआई-आधारित प्रणालियों की गुणवत्ता, विश्वसनीयता और अनुपालन सुनिश्चित कर सकता है। हालाँकि, किसी को यह ध्यान में रखना होगा कि सिस्टम के विकसित होने पर एआई विकास की पुनरावृत्तीय प्रकृति को निरंतर सत्यापन और अपडेट की आवश्यकता हो सकती है।

एआई में उन्नत IV&V का संभावित प्रभाव

एआई विकास में संवर्धित IV&V प्रक्रियाओं का एकीकरण एआई-आधारित प्रणालियों की गुणवत्ता, विश्वसनीयता और नैतिक विचारों को महत्वपूर्ण रूप से बढ़ाने की क्षमता रखता है। कुछ संभावित लाभ नीचे सूचीबद्ध हैं:

1. **प्रणालियों का बेहतर प्रदर्शन:** कठोर IV&V प्रक्रियाएं सुनिश्चित करती हैं कि AI मॉडल का पूरी तरह से परीक्षण और सत्यापन किया जाता है, जिससे

वास्तविक दुनिया के परिदृश्यों में बेहतर प्रदर्शन होता है। यह, बदले में, एआई अनुप्रयोगों में उपयोगकर्ता की संतुष्टि और विश्वास को बढ़ाता है।

2. **नैतिक और नियामक अनुपालन:** IV&V में नैतिक प्रभाव आकलन और गोपनीयता विचारों को शामिल करके, संगठन जिम्मेदार एआई विकास के प्रति प्रतिबद्धता प्रदर्शित कर सकते हैं। यह न केवल नियमों का अनुपालन सुनिश्चित करता है बल्कि उपयोगकर्ताओं और हितधारकों के बीच विश्वास को भी बढ़ावा देता है।

3. **जोखिम न्यूनीकरण:** IV&V के दौरान संभावित पूर्वाग्रहों, कमजोरियों और नैतिक चिंताओं की पहचान करना और उनका समाधान करना प्रतिकूल परिणामों के जोखिम को कम करता है। सक्रिय जोखिम शमन उपाय एआई-आधारित प्रणालियों की दीर्घकालिक सफलता और स्थिरता में योगदान करते हैं।

4. **निरंतर सुधार:** एआई विकास की पुनरावृत्तीय प्रकृति के लिए निरंतर सत्यापन और अद्यतन की आवश्यकता होती है। IV&V प्रक्रियाएं जो चल रही निगरानी, फीडबैक एकीकरण और अनुकूलन का समर्थन करती हैं, यह सुनिश्चित करती हैं कि AI सिस्टम समय के साथ प्रभावी और प्रासंगिक बने रहें।

निष्कर्ष

जैसे-जैसे एआई अनुप्रयोग प्रौद्योगिकी के भविष्य को आकार दे रहे हैं, एआई-आधारित प्रणालियों के सत्यापन से सम्बंधित अनूठी चुनौतियों का सामना करने के लिए पहले से बेहतर एवं मजबूत IV&V प्रक्रियाओं का एकीकरण अनिवार्य हो जाता है। जैसे-जैसे व्यवसाय/संगठन इन उन्नत IV&V प्रथाओं को अपनाते हैं, वे एआई समाधान देने के लिए तैयार हैं जो न केवल कार्यात्मक आवश्यकताओं को पूरा करते हैं बल्कि गुणवत्ता और नैतिक विचारों के उच्चतम मानकों का भी पालन करते हैं।

संदर्भ

1. इमैनुएल अमीसेन; "मशीन लर्निंग संचालित अनुप्रयोगों का निर्माण: विचार से उत्पाद तक जाना"
2. क्रिस्टोफ़ मोल्नार; "व्याख्यात्मक मशीन लर्निंग"
3. टिमनिट गेब्रू एट अल। "सोशियोटेक्निकल सिस्टम में निष्पक्षता और अमूर्तता", कंप्यूटर-मानव इंटरेक्शन पर एसीएम लेनदेन (TOCHI) (https://arxiv.org/abs/1604.03339)
4. इयान गुडफेलो एट अल। "डीप लर्निंग में प्रतिकूल हमले और बचाव", न्यूरल नेटवर्क और लर्निंग सिस्टम पर आईईईई लेनदेन [डीप लर्निंग में प्रतिकूल हमले और बचाव] (https://arxiv.org/abs/1801.08352)
5. आर्टिफिशियल इंटेलिजेंस पर यूरोपीय आयोग के उच्च-स्तरीय विशेषज्ञ समूह द्वारा "भरोसेमंद एआई के लिए नैतिक दिशानिर्देश" [भरोसेमंद एआई के लिए नैतिक दिशानिर्देश] (https://ec.europa.eu/digital-single-market/en/news/ethics)-दिशानिर्देश-भरोसेमंद-एआई)
6. अंतर्राष्ट्रीय मानकीकरण संगठन (आईएसओ) द्वारा "आईएसओ/आईईसी/आईईईई 29119 - सॉफ्टवेयर और सिस्टम इंजीनियरिंग - सॉफ्टवेयर परीक्षण" [आईएसओ/आईईसी/आईईईई 29119]

   (https://www.iso.org/standard/74549।एचटीएमएल)

FIDO2: पासवर्ड रहित प्रमाणीकरण मानक

श्रीमती अंशु भारद्वाज, वैज्ञानिक जी

प्रस्तावना

FIDO का मतलब फास्ट आइडेंटिटी ऑनलाइन है। FIDO2 का मुख्य उद्देश्य इंटरनेट पर पासवर्ड के उपयोग को ख़त्म करना है। इसे इंटरनेट पर सुरक्षित पासवर्ड रहित प्रमाणीकरण के लिए खुले और लाइसेंस-मुक्त मानकों को पेश करने के लिए विकसित किया गया था। पासवर्ड, और विरासत प्रमाणीकरण के अन्य रूप जैसे एसएमएस ओटीपी, ज्ञान-आधारित हैं, याद रखने में परेशानी होती है, और फ़िश करना, कटाई करना और दोबारा खेलना आसान है। 80% से अधिक डेटा उल्लंघनों का मूल कारण पासवर्ड हैं। उपयोगकर्ताओं के पास 90 से अधिक ऑनलाइन खाते हैं। 51% तक पासवर्ड का पुन: उपयोग किया जाता है। FIDO2 प्रमाणीकरण प्रक्रिया लॉगिन उपयोगकर्ता नाम और पासवर्ड के उपयोग से आने वाले पारंपरिक खतरों को समाप्त करती है, इसे FIDO2 लॉगिन मानक के साथ बदल देती है। इस प्रकार, यह फ़िशिंग और मैन-इन-द-मिडिल हमलों जैसे सामान्य ऑनलाइन हमलों से बचाता है।

परिचय

FIDO (फास्ट आइडेंटिटी ऑनलाइन) एलायंस एक खुला उद्योग मानक है जिसका मिशन पासवर्ड रहित प्रमाणीकरण प्रोटोकॉल बनाने का तरीका खोजना है। दिसंबर 2014 में, पहला पूर्ण FIDO पासवर्ड रहित प्रोटोकॉल जारी किया गया था। FIDO2 प्रोजेक्ट FIDO एलायंस और वर्ल्ड वाइड वेब कंसोर्टियम (W3C) के बीच एक संयुक्त प्रयास है जिसका लक्ष्य वेब के लिए मजबूत प्रमाणीकरण बनाना और ब्राउज़रों और वेब प्लेटफ़ॉर्म बुनियादी ढांचे में FIDO प्रमाणीकरण को मानकीकृत करना है। FIDO2 को आधिकारिक तौर पर अप्रैल 2018 में लॉन्च किया गया था, और इसे Google Chrome, मोज़िला फ़ायरफ़ॉक्स और Microsoft Edge में लागू किया गया था। 2020 में, iOS पर Safari, MacOS BigSur और iPad OS 14 ने FIDO2 के लिए समर्थन का विस्तार किया। FIDO2 उपयोगकर्ताओं को प्रमाणित करने के लिए एक पासवर्ड रहित तरीका प्रदान करता है और सुरक्षा, सुविधा, गोपनीयता और स्केलेबिलिटी समस्याओं का समाधान करता है जो पासवर्ड नहीं करते हैं। ऑनलाइन सेवाओं को एक मानक वेब एपीआई के माध्यम से एक्सेस किया जा सकता है, जिसे वेब प्लेटफ़ॉर्म इंफ्रास्ट्रक्चर में बनाया जा सकता है।

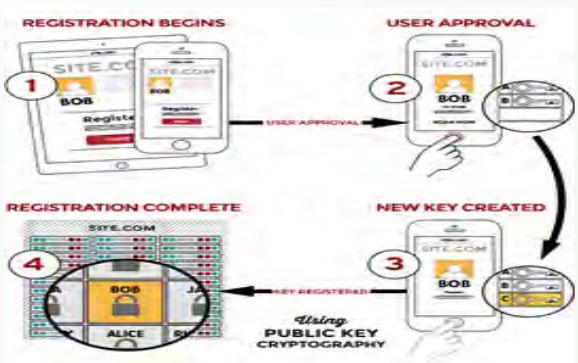
FIDO2 कैसे काम करता है?

यह मानक सुरक्षित और सुविधाजनक प्रमाणीकरण प्रणाली की गारंटी के लिए सार्वजनिक-कुंजी क्रिप्टोग्राफी का उपयोग करता है। इसे प्राप्त करने के लिए FIDO2 मानक प्रत्येक उपयोगकर्ता की पहचान को मान्य करने के लिए एक निजी और सार्वजनिक पासकी का उपयोग करता है।

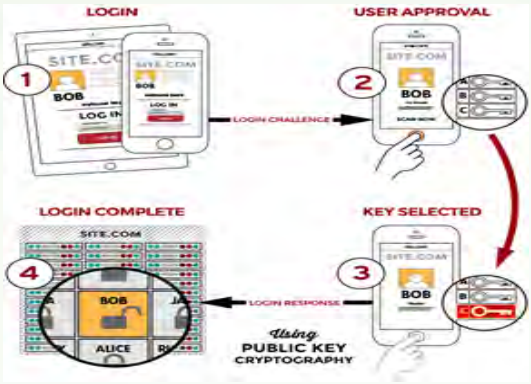
FIDO2 प्रमाणीकरण का उपयोग करने के लिए, पहला चरण पासवर्ड रहित साइन-इन सेट करना है:

1. एक FIDO2 प्रमाणक चुनें (या तो एक बाहरी प्रमाणक उपकरण या उपयोगकर्ता एजेंट के अंदर प्लेटफ़ॉर्म प्रमाणक)
2. सेवा एक FIDO2 प्रमाणीकरण कुंजी जोड़ी उत्पन्न करेगी।
3. FIDO2 प्रमाणक सार्वजनिक कुंजी को सेवा में भेजता है, जबकि संवेदनशील जानकारी वाली निजी कुंजी प्रमाणक पर रहती है।

एक बार सुरक्षित संचार पथ सक्षम हो जाने पर, सेटअप क्रेडेंशियल स्थायी रूप से संग्रहीत हो जाते हैं, जिससे बाद में लॉगिन की अनुमति मिलती है।



FIDO पंजीकरण



FIDO लॉगिन

*FIDOalliance.org से आरेख

अगली बार FIDO2 मानक का समर्थन करने वाली सेवाओं में से किसी एक में लॉग इन इस प्रकार किया जा सकता है:

1. उपयोगकर्ता को बायोमेट्रिक्स जानकारी का उपयोग करके पहचान करनी होगी
2. सेवा एक क्रिप्टोग्राफ़िक चुनौती देगी।
3. FIDO2 प्रमाणक निजी कुंजी का उपयोग करके चुनौती पर हस्ताक्षर करेगा
4. सेवा का सर्वर आपकी प्रतिक्रिया की पुष्टि करता है और आपको आपके खाते तक पहुंच प्रदान करता है। पंजीकरण प्रक्रिया के दौरान संग्रहीत संबंधित सार्वजनिक कुंजी का उपयोग कर हस्ताक्षर

FIDO2 के लाभ

1. FIDO2 किसी सर्वर पर क्रेडेंशियल संग्रहीत नहीं करता है और अद्वितीय क्रिप्टोग्राफ़िक लॉगिन क्रेडेंशियल का उपयोग करता है, जो फ़िशिंग, पासवर्ड चोरी और रीप्ले हमलों की संभावना को कम करने में मदद करता है।
2. इसके अलावा, इस सुरक्षित वेब लॉग-इन प्रक्रिया के लिए सर्वर के साथ किसी भी रहस्य का आदान-प्रदान नहीं किया जाता है। जानकारी का महत्वपूर्ण हिस्सा, यानी FIDO2 सुरक्षा कुंजी, हमेशा प्रमाणक पर ही रहती है।
3. इसके अतिरिक्त, यह उपयोगकर्ताओं के लिए सुविधाजनक है क्योंकि वे फिंगरप्रिंट और आईरिस स्कैनर, आवाज और चेहरे की पहचान जैसे बायोमेट्रिक बायोमेट्रिक्स के साथ-साथ मौजूदा समाधान और संचार मानकों, जैसे विश्वसनीय प्लेटफ़ॉर्म मॉड्यूल (टीपीएम), यूएसबी सुरक्षा टोकन, एम्बेडेड सुरक्षित तत्वों का लाभ उठाते हैं। (ईएसई), स्मार्ट कार्ड और नियर-फील्ड कम्युनिकेशन (एनएफसी)। जैसे फिंगरप्रिंट, चेहरा, आईरिस या लॉग इन करने के लिए साधारण FIDO2 सुरक्षा कुंजी।
4. अंत में, क्योंकि प्रत्येक वेबसाइट के लिए कुंजियाँ अद्वितीय होती हैं, उपयोगकर्ताओं को सभी साइटों पर ट्रैक नहीं किया जा सकता है।

निष्कर्ष

जैसे-जैसे उद्योग FIDO2 को अपनाना जारी रखता है, इसे अपनाना और आगे का विकास प्रमाणीकरण परिदृश्य को बदलने और व्यक्तियों और संगठनों के लिए ऑनलाइन सुरक्षा को मजबूत करने का वादा करता है।

संदर्भ:

1. https://fidoalliance.org/
2. https://en.wikipedia.org/wiki/FIDO_Alliance

क्लाउड कंप्यूटिंग में वर्चुअलाइजेशन (virtualization) की भूमिका

श्रीमती हेमलता बारी, वैज्ञानिक 'ई'

1. सारांश

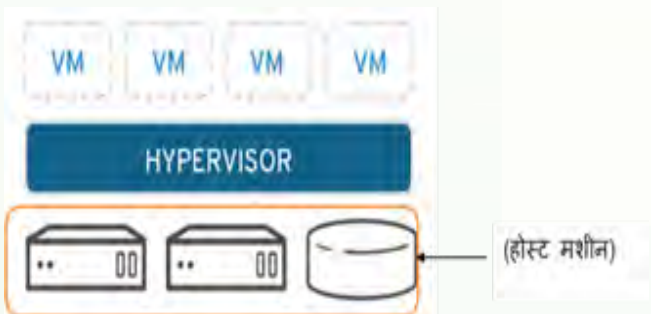
नवीन प्रौद्योगिकियों के द्वारा आईटी सेवाओं का उपयोग करना बहुत आसान हो गया हैं। वर्चुअलाइजेशन तकनीक से हार्डवेयर के संसाधनों का उपयोग करके उपयोगी सेवाएं प्रदान करता हैं। यह आपको एक मशीन की पूरी क्षमता का उपयोग करने की अनुमति देता है। यह लेख वर्चुअलाइजेशन के विभिन्न तकनीकों के बारे में वर्णन करता हैं ।

2. वर्चुअलाइजेशन कैसे काम करता हैं?

वर्चुअलाइजेशन तकनीक का आविष्कार सन् 1960 के आसपास आईबीएम द्वारा किया गया था। अपनी स्थापना के बाद से इसने लोगों के गणना करने के तरीके को बदलने में मदद की है। वर्चुअलाइजेशन एक ऐसी प्रक्रिया हैं, जो डेस्कटॉप, ऑपरेटिंग सिस्टम, नेटवर्क संसाधनों या सर्वर के वर्चुअल संस्करण के निर्माण को सक्षम बनाता है। क्लाउड कंप्यूटिंग में वर्चुअलाइजेशन एक महत्वपूर्ण भूमिका निभाता है।

वर्चुअलाइजेशन के तीन प्रमुख भाग:

- **होस्ट मशीन :** इस मशीन में ऑपरेटिंग सिस्टम इंस्टाल होता हैं । इस मशीन में सारे हार्डवेयर के संसाधन नियुक्त हुए होते हैं ।



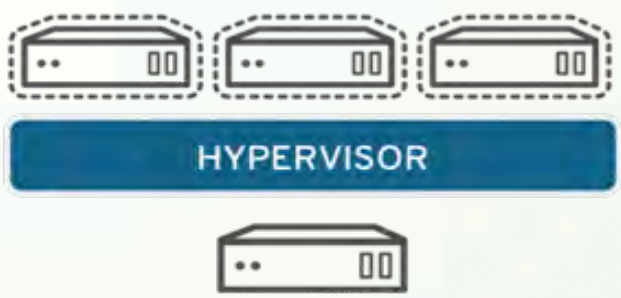
चित्र 1: वर्चुअलाइजेशन तकनीक

- **हाइपरवाइज़र(Hypervisor) :** यह सॉफ़्टवेयर भौतिक संसाधनों को वर्चुअल वातावरण से अलग करता है । हाइपरवाइज़र एक ऑपरेटिंग सिस्टम के ऊपर लेयर में काम करता हैं या सीधे हार्डवेयर पर भी इंस्टाल किए जा सकते हैं। हाइपरवाइज़र आपके भौतिक संसाधनों को लेते हैं और उन्हें विभाजित करते हैं ताकि वर्चुअल वातावरण उनका उपयोग कर सके।
- **वर्चुअल मशीन :** संसाधनों को आवश्यकता अनुसार भौतिक वातावरण से लेकर कई वर्चुअल वातावरण में विभाजित किया जाता है। उपयोगकर्ता जिस वर्चुअल वातावरण के भीतर गणना करते हैं, उसको वर्चुअल मशीन कहा जाता है। वर्चुअल मशीन एक डेटा फ़ाइल के रूप में कार्य करती है और किसी भी डिजिटल फ़ाइल की तरह, इसे एक कंप्यूटर से दूसरे कंप्यूटर में ले जाया जा सकता है, किसी एक में खोला जा सकता है और उम्मीद की जा सकती है कि यह उसी तरह काम करेगा।

3. क्लाउड कंप्यूटिंग में उपयोग होने वाले वर्चुअलाइजेशन तकनीक

a. सर्वर/ हार्डवेयर वर्चुअलाइजेशन

इसका मूल विचार, कई छोटे भौतिक सर्वरों को एक बड़े भौतिक सर्वर में व्यवस्थित करना है ताकि सिस्टम का अधिक प्रभावशाली ढंग से उपयोग किया जा सके। भौतिक सर्वर पर चलने वाला ऑपरेटिंग सिस्टम के द्वारा वर्चुअल मशीन बनाया जाता हैं जिस पर अलग अनुप्रयोग या सेवाएं प्रदान कर सकते हैं। किसी सर्वर को वर्चुअलाइज़ करने से यह उन विशिष्ट कार्यों को करने में सक्षम हो जाता है ।



चित्र 2: सर्वर वर्चुअलाइजेशन

b. डेटा वर्चुअलाइजेशन

हर जगह फैले डेटा को एक ही स्रोत में संगठित किया

जा सकता है, कई स्रोतों से डेटा को एक साथ ला सकता है, नए डेटा स्रोतों को आसानी से समायोजित कर सकता है, और उपयोगकर्ता की जरूरतों के अनुसार डेटा को बदल सकता है। डेटा वर्चुअलाइजेशन में अलग डेटा का स्रोत एक होता हैं यह किसी भी अनुप्रयोग या उपयोगकर्ता को सही समय पर आवश्यक डेटा - आवश्यक रूप में वितरित करते हैं।

चित्र 3:डेटा वर्चुअलाइजेशन

c. ऑपरेटिंग सिस्टम वर्चुअलाइजेशन

यह Linux और Windows को एक ही मशीन में, एक साथ चलाने का एक उपयोगी तरीका है। इसके लाभ निम्नलिखित हैं -

- हार्डवेयर लागत कम हो जाती है, क्योंकि कंप्यूटर को ऐसी उच्च आउट-ऑफ़-द-बॉक्स क्षमताओं की आवश्यकता नहीं होती है।
- सुरक्षा बढ़ जाती है, क्योंकि सभी वर्चुअल मशीन की निगरानी की जा सकती है और उन्हें अलग किया जा सकता है।
- सॉफ्टवेयर अपडेट जैसी आईटी सेवाओं पर खर्च कम होता हैं ।

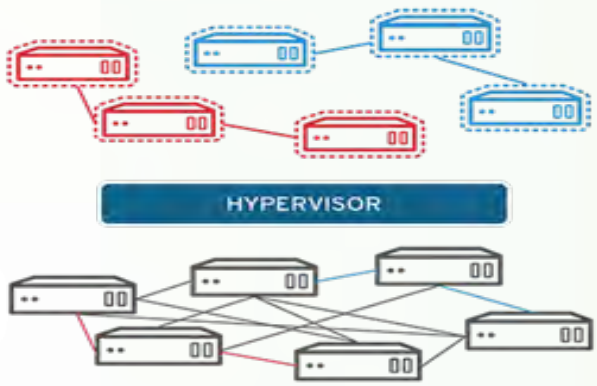
चित्र 4: ऑपरेटिंग सिस्टम वर्चुअलाइजेशन

d. नेटवर्क फ़ंक्शंस वर्चुअलाइजेशन

इससे कंप्यूटर नेटवर्क की निगरानी और नियंत्रण एक एडमिन मशीन से किया जा सकता हैं । इसका उद्देश्य नेटवर्क के डेटा ट्रांसफर दरों, स्केलेबिलिटी और सुरक्षा को अनुकूलन करना हैं। यह कई नेटवर्क प्रशासनिक कार्यों को भी स्वचालित करता है। नेटवर्क वर्चुअलाइजेशन विशेष रूप से उन नेटवर्कों के लिए उपयोगी हैं जो अप्रत्याशित ट्रैफ़िक वृद्धि का अनुभव करते हैं।

नेटवर्क वर्चुअलाइजेशन की दो श्रेणियां:

- आंतरिक: एक सिस्टम को नेटवर्क जैसी कार्यक्षमता प्रदान करना।
- बाहरी: कई नेटवर्क या नेटवर्क के कुछ हिस्सों को वर्चुअलाइजेशन करना।



चित्र 5: नेटवर्क फ़ंक्शंस वर्चुअलाइजेशन

4. वर्चुअलाइजेशन के लाभ

वर्चुअलाइजेशन के कुछ लाभ यहां दिए गए हैं:

- वर्चुअलाइजेशन कई लाभ प्रदान करता है, जैसे यह लागत में कमी और विकास प्रक्रिया की उत्पादकता को बढ़ाने में मदद करता है।
- यह अत्यधिक जटिल आईटी बुनियादी ढांचे की आवश्यकता को दूर करता है।
- यह सिस्टम विफलताओं के संदर्भ में शामिल जोखिमों को दूर करता है, और यह विभिन्न वर्चुअल सर्वरों के बीच डेटा स्थानांतरण को भी बढ़ावा देता है।
- वर्चुअलाइजेशन में काम करने की प्रक्रिया अत्यधिक प्रभावशाली है, जो यह सुनिश्चित करती है कि उपयोगकर्ता सबसे किफायती तरीके से काम करें और संचालित करें।

5. वर्चुअलाइजेशन के नुकसान

वर्चुअलाइजेशन के नुकसान साधारणतः बहुत सीमित हैं। वर्चुअलाइजेशन के नुकसान निम्नलिखित हैं:

- मौजूदा हार्डवेयर सेटअप को वर्चुअलाइज्ड सेटअप में बदलने के लिए व्यापक समय निवेश की आवश्यकता होती है।
- मौजूदा या वास्तविक सेटअप को वर्चुअल सेटअप में बदलने की कीमत महंगा होता हैं।

6. निष्कर्ष

वर्चुअलाइजेशन क्लाउड में वर्चुअल सर्वर को स्थापित करने का एक आसान तरीका प्रदान करता है, इसलिए आपको बहुत सारे संसाधानों की आवश्यकता नहीं होती है पर वर्चुअल संसाधनों का उपयोग कैसे किया जा रहा हैं, इस पर नज़र रखना महत्वपूर्ण है। कंपनी को पॉलिसी के द्वारा नियंत्रण करना चाहिए। वर्चुअलाइजेशन उत्पादकता, दक्षता तथा सुरक्षा प्रदान करता हैं, इसलिए लगातार लोकप्रियता हासिल कर रहा है।

स्टेल्थ फ़ायरवॉल: गोपनीय नेटवर्क सुरक्षा का एक अद्‌त कवच

श्री रविशंकर यादव, वै 'एफ'

सारांश

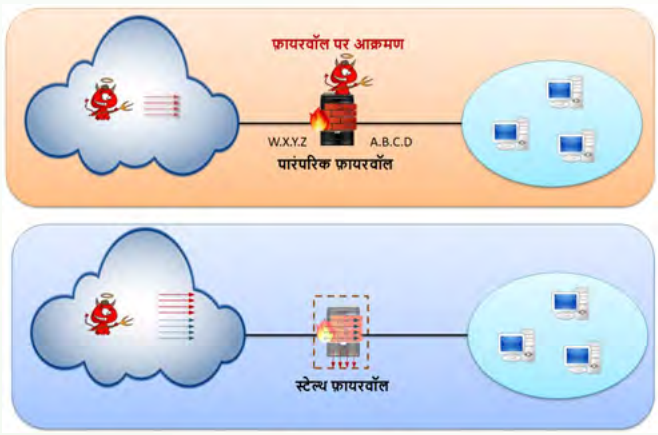
आधुनिक तकनीकी युग में साइबर जुर्म के बढ़ते हुए खतरों से कोई भी अनभिज्ञ नहीं है। इंटरनेट पर संचार और संबंधित वेब संचार तेजी से बढ़ रहा है, जिससे साइबर सुरक्षा की आवश्यकता बढ़ रही है। फ़ायरवॉल नेटवर्क सुरक्षा के महत्वपूर्ण स्तंभों में से एक है। पारंपरिक नेटवर्क फ़ायरवॉल आईपी दृश्यमान (विजिबिल) होने के कारण नेटवर्क-आधारित हमले के प्रति संवेदनशील होते हैं। आईपी दृश्यमान फ़ायरवॉल अविश्वसनीय बाहरी नेटवर्क के साथ-साथ विश्वसनीय आंतरिक नेटवर्क में उपस्तिथ हमलावरों द्वारा आईपी (इन्टरनेट प्रोटोकॉल) सम्पर्क योग्य होते हैं। यदि कोई हमलावर फ़ायरवॉल में सेंध लगाने और उसे पुन: कॉन्फ़िगर करने में सफल हो जाता है तो नेटवर्क सुरक्षा के लिए गंभीर स्थिति उत्पन्न हो सकती है। इस स्तिथि में, हमलावर या तो कुछ विशिष्ट नेटवर्क सेवा को, स्वयं को प्रयोग करने की अनुमति प्रदान करने के लिए फ़ायरवॉल को पुन: विन्यासित (कॉन्फ़िगर) कर सकता है| अथवा हमलावर फ़ायरवॉल को पुन: विन्यसित (कॉन्फ़िगर) कर पूरे निजी नेटवर्क को किसी के भी पहुंच योग्य बना सकता है। इस स्तिथि मैं सबसे बड़ा जोखिम यह है कि फ़ायरवॉल मैं एक बार सेंध लगाने के बाद साइबर सुरक्षा के परिपेक्ष से बहुत ही गंभीर स्तिथि उत्पन्न हो जाती है और पूरा नेटवर्क हमलावर की दया पर निर्भर हो जाता है। आईपी दृश्यता के कारण उत्पन्न गंभीर सुरक्षा संबंधी चिंताओं को दूर करने के लिए, हमने एक स्टेल्थ (गोपनीय) पैकेट फ़िल्टरिंग फ़ायरवॉल का निर्माण किया है। स्टेल्थ फ़ायरवॉल एक नई पीढ़ी की फ़ायरवॉल है जो साइबर सुरक्षा को एक नए स्तर पर ले जाता है। यह एक उन्नत सुरक्षा कवच है जो साइबर अपराधियों के खिलाफ एक गोपनीय ढाल प्रदान करता है। इसे "स्टेल्थ" कहा जाता है क्योंकि यह अपने काम को छिपाता है और साइबर अपराधियों को इसका अनुमान भी नहीं होता है। यह साइबर अपराधियों को धोखा देता है और अनुमानित हमलों को रोकने में सक्षम होता है| इस फ़ायरवॉल का निर्माण हमने लिनक्स ऑपरेटिंग सिस्टम पर किया | यह शोध पत्र में पारंपरिक फ़ायरवॉल की खामियों को दूर करने के लिए स्टेल्थ फ़ायरवॉल निर्माण के हमारे दृष्टिकोण, स्टेल्थ फ़ायरवॉल की लिनिक्स ऑपरेटिंग सिस्टम पर निर्माण विधि, इसके कार्य के विविध पहलुओं का वर्णन और इसका निष्पादन मूल्यांकन (परफॉरमेंस इवैल्यूएशन) प्रस्तुत किया गया है|

1 प्रस्तावना

तेजी से बदलती प्रौद्योगिकी के साथ, अधिकांश संगठनों के लिए, बाहरी दुनिया से जुड़ना और अपने महत्वपूर्ण नेटवर्क संसाधनों से समझौता किए बिना सूचनाओं का आदान-प्रदान करना एक गंभीर चुनौती है और भविष्य में भी रहेगी। जब नेटवर्क एक साथ जुड़े होते हैं, तो जुड़े हुए विभिन्न पक्षों में अक्सर विश्वास के विभिन्न स्तर (ट्रस्ट लेवेल्स) मौजूद होते हैं। नेटवर्क मैं कंप्यूटरों को परिवर्तनीय विश्वास (ट्रांजिटिव ट्रस्ट) की समस्या का सामना करना पड़ता हैं [1]। फ़ायरवॉल नेटवर्क सुरक्षा का एक अग्रणी रक्षा तंत्र है [2]। फ़ायरवॉल नेटवर्क में आने या जाने वाले अवांछित नेटवर्क ट्रैफ़िक को फ़िल्टर करके आतंरिक और विस्वसनीय नेटवर्क को हमले और अनधिकृत पहुंच से सुरक्षा प्रदान करता है [3]। फ़ायरवॉल नेटवर्कों को विस्वस्ता (ट्रस्ट लेवेल्स) के आधार पर अलग-अलग सीमांकित करता है और सुरक्षा नीति (पोलिसी) के अनुसार नेटवर्कों के बीच नेटवर्क ट्रैफ़िक में मध्यस्थता करता है।

फ़ायरवॉल विभिन्न प्रकार के होते हैं| फ़ायरवॉल का चुनाव सुरक्षा नीति की आवस्यकता और नेटवर्क सिस्टम में परिनियोजन (डिप्लॉयमेंट) के स्तर पर निर्भर करता है। पैकेट फ़िल्टरिंग फ़ायरवॉल [1] प्रख्यात फ़ायरवॉल प्रणालियों में से एक है जो कि ओएसआई मॉडल की ट्रांसपोर्ट परत (लेयर) पर काम करता है। नेटवर्क सुरक्षा के लिए पैकेट फ़िल्टरिंग की शुरुआत मोगुल (Mogul) के पेपर अबाउट स्क्रीनड [4] से हुई थी। पैकेट फ़िल्टरिंग फ़ायरवॉल आंतरिक नेटवर्क और बाहरी नेटवर्क के मध्य एक जाँच विन्द (चेकपॉइंट) के रूप में कार्य करता है| उदाहरण के लिए, इंट्रानेट और इंटरनेट के बीच। पैकेट फ़िल्टरिंग फ़ायरवॉल आमतौर पर गेटवे या राउटर में लागू किया जाता है। इस

फ़ायरवॉल में, फ़ायरवॉल पर आने वाले प्रत्येक आईपी डेटाग्राम को टीसीपी/आईपी पैकेट हेडर मैं उपस्तिथ सूचनाओं के आधार पर निर्दिष्ट नियमों के अनुसार फ़िल्टर किया जाता है [1, 5]। इस तंत्र को तैयार करने में, फ़ायरवॉल सिस्टम में कम से कम दो आईपी एड्रेस की आवस्यकता होती है। साथ ही, फ़ायरवॉल सिस्टम को आंतरिक नेटवर्क के सभी उपयोगकर्ताओं के लिए गेटवे के रूप में विन्यासित (कॉन्फ़िगर) करना पड़ता है। यह पैकेट फ़िल्टरिंग फ़ायरवॉल को आंतरिक और बाह्य दोनों नेटवर्क से आईपी दृश्यमान (विज़िबल) बना देता है। नेटवर्क में फ़ायरवॉल की आईपी दृश्यता पैकेट फ़िल्टरिंग फ़ायरवॉल सिस्टम को नेटवर्क-आधारित हमलों के प्रति संवेदनशील बना देती है।आईपी दृश्यमान फ़ायरवॉल को कई तरीकों से भेदा जा सकता है, और परिणामी क्षति का अनुमान लगाना बेहद मुश्किल होता है [6, 7]। किसी फ़ायरवॉल को भेदने का एक तरीका सीधे उसी पर हमला करके उसे ही लक्षित (टारगेट) करना है। चूंकि पैकेट फ़िल्टरिंग फ़ायरवॉल आईपी पहुंच योग्य होते है, एक हमलावर उपयोगी जानकारी निकालने के लिए नेटवर्क के सभी दृश्यमान संसाधनों जिसमें फ़ायरवॉल भी सामिल है, की जांच (प्रोब), स्कैन और भेद्यता योग्य खामियों का पता लगा सकता है, जैसा के चित्र -1 मैं दर्शया गया है। इस एकत्रित जानकारी का उपयोग हमलावर द्वारा फ़ायरवॉल सिस्टम और नेटवर्क को भेदने के लिए किया जाता है| इसलिए, फ़ायरवॉल को न केवल नेटवर्क की बल्कि स्वयं को भी सुरक्षित रखने की अत्यन्त आवश्यकता होती है।



चित्र-1, हमलावर के परिपेक्ष से पारंपरिक और स्टेल्थ फ़ायरवॉल

आईपी दृश्यता के कारण इस सुरक्षा भेद्यता को संबोधित करने के तरीकों में से एक नेटवर्क में आईपी दृश्यता के बिना पैकेट फ़िल्टरिंग फ़ायरवॉल की कल्पना करना है। जैसा के चित्र -1 मैं दर्शया गया है, एक गोपनीय (स्टेल्थ) फ़ायरवॉल जो की हमवारों के लिए अद्रश्यमान हो| इस कल्पना को पूरा करने के लिए सबसे महत्वपूर्ण, बिना आईपी एड्रेस के फ़ायरवॉल का निर्माण करना है| इसको हासिल करने के लिए हमने आंतरिक और बाहरी नेटवर्क को जोड़ने के लिए आईपी गेटवे के बजाय नेटवर्क ब्रिजिंग का उपयोग किया। नेटवर्क ब्रिज [8] के रूप में निर्मित फ़ायरवॉल सिस्टम ओएसआई मॉडल की डेटा लिंक परत (लेयर) पर काम करता है और इसलिए इसे आईपी एड्रेस की आवश्यकता नहीं होती है। यह फ़ायरवॉल नेटवर्क में आईपी अदृश्य (इनविजिबल) होते हैं और इसलिए इसे स्टेल्थ फ़ायरवॉल माना जाता है। लिनक्स कर्नल नेटफिल्टर [9] नामक एक शक्तिशाली पैकेट फ़िल्टरिंग ढांचा प्रदान करता है। नेटफ़िल्टर फ्रेमवर्क एक पैकेट फ़िल्टर फ़ायरवॉल सिस्टम को लागू करने के लिए नेटवर्क पैकेट को इंटरसेप्ट करने और नेटवर्क पैकेट मैं बदलाब करने के लिए हुक प्रदान करता है। हमने नेटफिल्टर के साथ ब्रिज-एनएफ इंफ्रास्ट्रक्चर [10] का उपयोग करते हुए एक फ़ायरवॉल तैयार किया जिसमें नेटफिल्टर की सभी पैकेट फ़िल्टरिंग क्षमताओं का उपयोग किया जा सकता है। हमने एक ऐसे फ़ायरवॉल सिस्टम का निर्माण किया है जो की तैनाती में आसान और बेहतर फ़िल्टरिंग क्षमताओं के अतिरिक्त लाभों के साथ-साथ गुप्त (स्टेल्थ) रहने की क्षमता भी रखता है।

इस परिचयात्मक खंड के बाद, इस प्रपत्र का शेष भाग निम्नानुसार व्यवस्थित किया गया है: अनुभाग 2 में संबंधित प्रकाशित कार्य पर चर्चा, अनुभाग 3 में फ़ायरवॉल प्लेटफ़ॉर्म के रूप में लिनक्स के बारे में विवरण, अनुभाग 4 में हमारे दृष्टिकोण अनुभाग 5 में कार्यान्वयन की व्याख्या, अनुभाग 6 में निष्पादन मूल्यांकन हेतु प्रयोग और परिणाम तथा अनुभाग 7 में निष्कर्ष के साथ यह शोध पत्र समाप्त होता है।

2 संबंधित प्रकाशित कार्य

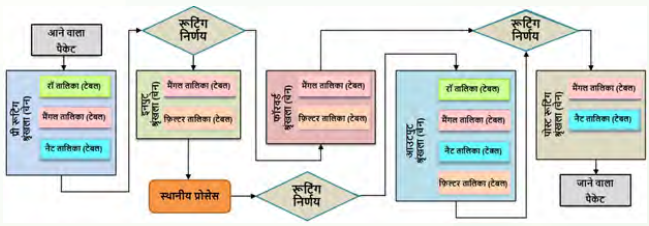
फ़ायरवॉल लगभग 1987 से अस्तित्व में हैं, इसे कार्यान्वित करने के लिए अब तक विभिन्न तरीकों को आज़माया गया है। कहन (Kahn) इत्यादी ने 1997 में पहली बार ब्रिज मोड में फ़ायरवॉल कार्यान्वयन की शुरुआत की और DOS ऑपरेटिंग सिस्टम वाले कंप्यूटरों के लिए फ़ायरवॉल विकसित किया [7]। 1999 में जियानबिंग लियू (Jianbing Liu) और यान मा (Yan Ma) ने भी अपने पेपर में इस दृष्टिकोण का वर्णन किया [11] ।

केरोमाइटिस (Keromytis) और राइट (Wright) ने सुरक्षित, वर्चुअल लेंन (VLAN) स्थापित करने के लिए ब्रिजिंग फ़ायरवॉल के प्रयोग की चर्चा की [12]। अन्य संबंधित कार्य लिनक्स मशीन को नेटवर्क ब्रिज के रूप में स्थापित करने के लिए कार्यान्वयन गाइड के रूप में उपलब्ध हैं। हालाँकि, स्टेल्थ फ़ायरवॉल निर्माण के क्षेत्र में बहुत अधिक शोध का काम नहीं किया गया है और हमारे जानकारी के अनुसार लिनक्स नेटफिल्टर का प्रोयोग करके स्टेल्थ फ़ायरवॉल के निर्माण के शोध हमने पहली बार प्रस्तुत किया है ।

3 लिनक्स फ़ायरवॉल प्लेटफ़ॉर्म के रूप में

लिनक्स (Linux) में नेटफ़िल्टर-आधारित एक शक्तिशाली पैकेट फ़िल्टर फ्रेमवर्क शामिल रहता है और इसने एक उत्कृष्ट फ़ायरवॉल फ्रेमवर्क प्लेटफ़ॉर्म के रूप में ख्याति प्राप्त की हुई है। नेटफिल्टर फ्रेमवर्क की शुरुआत 1998 में रस्टी रसेल (Rusty Russell) द्वारा पुराने लिनक्स संस्करणों में उपयोग किए गए आईपी फ़िल्टरिंग के पहले के रूपों में सुधार के रूप में की गई थी [9]। इनमें लिनक्स 2.0 में आईपीएफडब्लूएडम (ip-fwadm) और लिनक्स 2.2 में आईपीचेन्स (IPChains) शामिल हैं। नेटफिल्टर से पहले, लिनक्स कर्नेल में सामान्य पैकेट नियंत्रण ढांचे का अभाव था। लिनक्स नेटफिल्टर पैकेट फ़िल्टर फ्रेमवर्क के पैकेट नियंत्रण ढांचे का मुख्य भाग इसका हुक प्रणाली (सिस्टम) है | लिनक्स नेटफिल्टर हुक प्रणाली (सिस्टम) के महत्वपूर्ण घटक ip_tables, ip6_tables, arp_tables और ebtables कर्नेल मॉड्यूल हैं [13]। फ़ायरवॉल नीति (पॉलिसी) को परिभाषित करने के लिए, नेटफ़िल्टर फ्रेमवर्क एक तालिका (टेबल) आधारित प्रणाली प्रदान करता है, जिसके आधार पर नेटवर्क पैकेट को फ़िल्टर या रूपांतरित किया जाता है। यूजरस्पेस अपलिकेशन iptables, ip6tables, arptables और ebtables इन तालिकाओं (टेबलस) के विन्यास (कॉन्फ़िगरेशन) और प्रशासन की सुविधा प्रदान करते हैं। भले ही iptables, ip6tables, arptables और ebtables कर्नेल मॉड्यूल और यूजरस्पेस अपलिकेशन दोनों के नाम समान हैं, उनमें से प्रत्येक अलग-अलग कार्यक्षमता वाली एक अलग इकाई है।

नेटफिल्टर फ्रेमवर्क कर्नेल के पैकेट प्रोसेसिंग मार्ग में पांच हुक बिंदुओं को परिभाषित करता है [13] जो लिनक्स कर्नेल के हेडर फ़ाइल /usr/include/linux/netfilter_ipv4.h में परिभाषित है। आईपी नेटवर्क स्टैक के माध्यम से जाने वाले नेटवर्क पैकेट इन हुकों द्वारा अवरोधित (इंटरसेप्ट) किए जाते हैं और पैकेट परसंस्करण (प्रोसेसिंग) के लिए निर्धारित नियमों से गुजरते हैं। नेटफ़िल्टर मवर्क इन पैकेट परसंस्करण (प्रोसेसिंग) नियमों को तालिकाओं (टेबलस) में व्यवस्थित करता है और इनमें से प्रत्येक तालिका एक विशिष्ट उद्देश्य को पूरा करती है। तालिकाओं को पैकेट परसंस्करण कार्य (प्रोसेसिंग फ़ंक्शंस) के आधार पर समूहीकृत किया जाता है, यानी, नेट, मैंगल, फ़िल्टर इत्यादि। फ़िल्टर, मैंगल, नेट, रॉ और सिक्योरिटी नेटफ़िल्टर फ्रेमवर्क की पाँच अंतर्निहित तालिकाएँ हैं [5, 9]। हालाँकि इन तालिकाओं को पैकेट प्रोसेसिंग फ़ंक्शंस द्वारा परिभाषित किया गया है, परन्तु अंतर्निहित श्रृंखलाएं (चेन्स) नेटफ़िल्टर हुक का प्रतिनिधित्व करती हैं जो उन्हें कार्य के लिए शुरु करती हैं। प्रत्येक तालिका में अंतर्निहित श्रृंखलाओं (चेन्स) का अपना समूह होता है [5,9]। नेटफिल्टर के माध्यम से नेटवर्क पैकेट का विभिन्न श्रृंखलाओं से होते हुए जाना चित्र 2 में दिखाया गया है। श्रृंखला (चेन) मूल रूप से यह निर्धारित करती है कि पैकेट प्रसंस्करण नियमों का मूल्यांकन कब किया जाएगा। ये श्रृंखलाएँ संबंधित नेटफ़िल्टर हुक द्वारा चालू होती हैं और उनके नामों को प्रतिबिंबित करती हैं। नेटफ़िल्टर ढाँचा पाँच अंतर्निर्मित श्रृंखलाओं के साथ आता है जैसा कि चित्र 2 [5, 9] में दर्शाया गया है। नेटफ़िल्टर उल्लिखित पैकेट परसंस्करण कार्य (प्रोसेसिंग फ़ंक्शंस) के साथ-साथ भार संतुलन (लोड बैलेंसिंग), रूपांतरण (मास्करेडिंग), पोर्ट फ़ॉरवर्डिंग, कनेक्शन ट्रैकिंग, अकाउंटिंग के लिए भी सहायता प्रदान करता है [14]। नेटफ़िल्टर फ्रेमवर्क में कस्टम हुक को पंजीकृत करने का प्रावधान रहता है अतः नेटफ़िल्टर फ्रेमवर्क का कस्टम हुक के कार्यान्वयन द्वारा आवश्यकता अनुसार विस्तार किया जा सकता है [13]।



चित्र-2, नेटफिल्टर फ्रेमवर्क कर्नेल के पैकेट परसंस्करण (प्रोसेसिंग) मार्ग

4 फ़ायरवॉल को स्टेल्थ बनाने की लिए हमारा दृष्टिकोण

एक पारंपरिक पैकेट फ़िल्टरिंग फ़ायरवॉल किसी भी नेटवर्क में सतह (लेयर) 3 उपकरण की तरह कार्य करता है और आंतरिक नेटवर्क और बाहरी नेटवर्क के बीच जाने वाले कंप्यूटर नेटवर्क ट्रैफ़िक का निरीक्षण करता है। यह पैकेट फ़िल्टरिंग फ़ायरवॉल एक रूटेड हॉप (routed hop) होता है और सभी आंतरिक नेटवर्क होस्ट के लिए एक डिफ़ॉल्ट गेटवे के रूप में विन्यासित (कॉन्फ़िगर) किया जाता है। इस तरह के सभी पैकेट फ़िल्टरिंग फ़ायरवॉल आंतरिक और बाहरी दोनों नेटवर्क से आईपी दृश्यमान होते हैं| किसी भी प्रकार के हमले मैं सबसे पहला और महत्वपूर्ण कदम अपने दुश्मन के बारे मैं जानकारी एकत्रित करना होता है [15]। एक हमलावर सर्वप्रथम नेटवर्क के सभी दृश्यमान संसाधनों की जांच, स्कैन और सुरक्षा खामियों की गणना करता है। इशी कारणवश आईपी दृश्यता इस प्रकार के पारंपरिक पैकेट फ़िल्टरिंग फ़ायरवॉल को नेटवर्क-आधारित हमलों के प्रति संवेदनशील बनाती है। इस सुरक्षा खामि के अलावा, किसी मौजूदा नेटवर्क में लेयर-3 पैकेट फ़िल्टरिंग फ़ायरवॉल को तैनात (डेपलॉय) करने के लिए नेटवर्क को पुन: विन्यासित (कॉन्फ़िगरेशन) करने की आवश्यकता पड़ती है, जिसमें बहुत समय और संसाधन की जरूरत होती है है| इसके अलावा नेटवर्क मैं कई विन्यास (कॉन्फ़िगरेशन) सम्बंधित समस्याएं भी आ सकती हैं [11, 12]।

आईपी दृश्यता के कारण इस सुरक्षा भेद्यता (वनरेविलिटी) को संबोधित करने के लिए, फ़ायरवॉल को इस तरह से डिज़ाइन किया जाना चाहिए कि फ़ायरवॉल को आईपी एड्रेस की आवश्यकता ही न हो। आईपी दृश्यता सम्बंधित सुरक्षा भेद्यता (वनरेविलिटी) को दूर करने के लिए हमारा दृष्टिकोण ओएसआई मॉडल में आई पी लेयर के स्थान पर एक लेयर नीचे, परत-2 (डाटा लिंक लेयर) पर फ़ायरवॉल की कल्पना करना है। हमने अपने फ़ायरवॉल को नेटवर्क ब्रिज डिवाइस [16,17] के रूप में डिज़ाइन किया है जो लेयर-2 पर काम करता है| चूंकि लेयर-2 डिवाइस मैक एड्रेस के आधार पर पैकेट अग्रेषित करता है और इसलिए इन्हें आईपी एड्रेस की आवश्यकता नहीं होती है।यह ब्रिज फ़ायरवॉल नेटवर्क मैं अदृश्य रूप मैं काम करता है अतः नेटवर्क से जुड़े हुए डिवाइसों के लिए यह राउटर हॉप के रूप में दिखाई नहीं देता है। चूंकि यह ब्रिज फ़ायरवॉल नेटवर्क में आईपी अदृश्य होता है, इसलिए इसे स्टेल्थ फ़ायरवॉल कहा जाता है।

5 स्टेल्थ फ़ायरवॉल का कार्यान्वयन

सभी प्रमुख लिनक्स वितरण पर नेटवर्क ब्रिजिंग का कार्यान्वयन किया जा सकता है। सामान्यतः जब फ़ायरवॉल ब्रिज रूप मैं कार्य करता है इसमें नेटवर्क पैकेट फ़ायरवॉल नेटवर्क स्टैक के लेयर-2 पर परसंस्करित (प्रोसेस) होता है| जैसा की चित्र-3 में दर्शाया गया है| ब्रिज फ़िल्टर (ईबीटेबल्स [10]), एक लेयर-2 पैकेट फ़िल्टर जो विशेष रूप से ईथरनेट ब्रिज के लिए डिज़ाइन किया गया है को कार्यान्वित करता है, ताकि लेयर-2 हेडर फ़ील्ड के आधार पर नेटवर्क ट्रैफ़िक को फ़िल्टर किया जा सके| ब्रिज फ़िल्टर (ईबीटेबल्स),) लिनक्स ब्रिज से गुजरने वाले नेटवर्क ट्रैफ़िक की पारदर्शी फ़िल्टरिंग को सक्षम बनाता है।

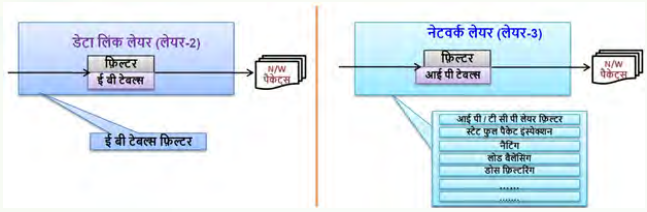
चित्र-3, फ़ायरवॉल ब्रिज रूप मैं नेटवर्क पैकेट परसंस्करण (प्रोसेसिंग) मार्ग

जब फ़ायरवॉल सामान्य गेटवे रूप मैं कार्य करता है मैं नेटवर्क पैकेट नेटवर्क स्टैक के लेयर-3 पर नेटफिल्टर फ़िल्टरिंग फ्रेमवर्क मैं परसंस्करित (प्रोसेस) होता है जैसा की चित्र-4 में दर्शाया गया है| नेटफिल्टर फ़िल्टरिंग फ्रेमवर्क मैं परसंस्करित होने के कारण फ़ायरवॉल के इस रूप मैं फ़िल्टरिंग की बहुत उन्नत छमतायें उपलब्ध हो जाती हैं |

चित्र-4, फ़ायरवॉल गेटवे रूप रूप में नेटवर्क पैकेट परसंस्करण (प्रोसेसिंग) मार्ग

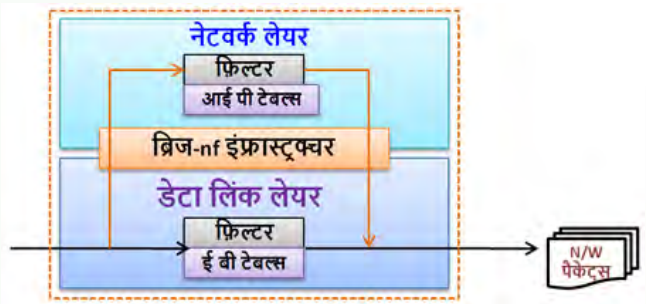
चित्र-5 मैं फ़ायरवॉल के लेयर-2 और लेयर-3 क्षमताओं को दर्शाया गया है| जैसा की चित्र-3 और चित्र-5 से विदित है की फ़ायरवॉल ब्रिज रूप मैं स्टेल्थ तो हो जाती है परन्तु इसमें नेटफिल्टर फ़िल्टरिंग फ्रेमवर्क में ब्रिज किए गए आईपीवी-4 पैकेट को पहुंचने की क्षमता नहीं होती है | अतः इसके पास केवल ब्रिज फ़िल्टर (ई बी टेबल्स) की क्षमता ही उपलब्ध रहती है| इसके बिपरीत जब फ़ायरवॉल सामान्य गेटवे रूप मैं कार्य करता है इसके पास फ़िल्टरिंग के बहुत सी क्षमताएं

उपलब्ध रहती हैं जैसा की चित्र-5 मैं दर्शाया गया है, परन्तु फ़ायरवॉल अपने इस रूप में नेटवर्क में खुद को हमलावरों केआखों से छुपा नहीं पता |



चित्र-5, नेटफिल्टर फ़िल्टरिंग फ्रेमवर्क के लेयर-2 और लेयर-3 क्षमताओं की तुलना

लिनक्स कर्नेल के नेटवर्क स्टैक मैं नेटफिल्टर फ़िल्टरिंग फ्रेमवर्क में ब्रिज किए गए आई पी वी-4 (IPv4) पैकेट को पहुंचने की क्षमता नहीं होतो है| हमने फ़ायरवॉल के ब्रिज रूप के स्टेल्थ और सामान्य गेटवे रूप के उन्नत फ़िल्टरिंग क्षमताओं के साथ मैं लाने के लिए एक लिनक्स कर्नेल मॉड्यूल (ब्रिज-एनएफ इंफ्रास्ट्रक्चर)का निर्माण किया जो ब्रिज रूप के सारे पैकेट्स को उच्च लेयरों तक पहुचता है और पैकेट परसंस्करण (प्रोसेसिंग) के बाद पुनः लेयर-२ पर पंहुचा देता है, जैसा की चित्र-6 मैं दर्शाया गया है |



चित्र-6, ब्रिज-एनएफ इंफ्रास्ट्रक्चर लिनक्स कर्नेल मॉड्यूल

ब्रिज इंटरफ़ेस पर नेटफ़िल्टर फ्रेमवर्क स्थापित करने से ब्रिज एक प्रभावशाली पैकेट फ़िल्टरिंग फ़ायरवॉल बन जाता है। आईपीटेबल्स की तुलना में, ईबीटेबल्स फ़िल्टरिंग संभावनाएं लिंक लेयर फ़िल्टरिंग और उच्च नेटवर्क परतों पर कुछ बुनियादी फ़िल्टरिंग तक सीमित हैं। ब्रिज फ़ायरवॉल सिस्टम में उच्च परतों पर आधारित उन्नत फ़िल्टरिंग क्षमताओं को शामिल करने के लिए, आईपीटेबल्स फ़िल्टरिंग टूल की आवश्यकता है [10]। ब्रिज को आईपीटेबल्स की सभी क्षमताओं के साथ एक शक्तिशाली पैकेट फ़िल्टरिंग सिस्टम के रूप में बनाने के लिए, हम ब्रिज-एनएफ इंफ्रास्ट्रक्चर [10] का लाभ उठाते हैं। ब्रिज-एनएफ इंफ्रास्ट्रक्चर लिनक्स कर्नेल की पहले से निर्मित ब्रिजिंग कार्यक्षमता का विस्तार करता है।

हमारे द्वारा निर्मित यह कर्नल मॉड्यूल एक सेकंड मैं पचास लाख पैकेट्स परसंस्करित (प्रोसेसिंग) कर सकता है| जैसा की चित्र-7 मैं दर्शाया गया है, यह कर्नल मॉड्यूल लिनक्स कर्नेल की पहले से निर्मित ब्रिजिंग फ़िल्टरिंग कार्यक्षमता का विस्तार करके इसके छमताओं को कई गुणा बड़ा कर इसमें चार चाँद लगा देता है |

चित्र-7, ब्रिज-एनएफ इंफ्रास्ट्रक्चर के द्वारा ब्रिजिंग फ़िल्टरिंग कार्यक्षमता का विस्तार

हमारे स्टेल्थ फ़ायरवॉल कार्यान्वयन में, हमने पारंपरिक पैकेट की सभी क्षमताओं वाले पैकेट फ़िल्टरिंग सिस्टम का निर्माण करने के लिए आईपीटेबल्स और ईबी टेबल्स के साथ ब्रिज-एनएफ बुनियादी ढांचे का उपयोग किया। हमारे द्वारा निर्मित इस स्टेल्थ फ़ायरवॉल को किसी भी नेटवर्क मैं अन्य उपकरणों, जिसकी वह सुरक्षा कर रहा है के साथ इन-लाइन प्लग किया जा सकता है ।

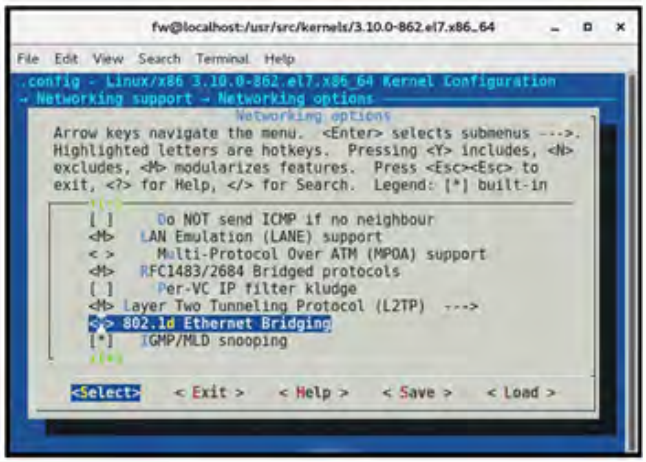
हमने इस स्टेल्थ फ़ायरवॉल को बनाने के लिए लिनक्स कर्नेल संस्करण 3.10.0-862 के साथ सेंटओएस (CentOS) लिनक्स रिलीज़ 7.5.1804 का उपयोग किया है। हमारे स्टेल्थ फ़ायरवॉल को बनाने करने की मुख्य प्रक्रियाएँ, एक नेटवर्क ब्रिज स्थापित करना और पैकेट फ़िल्टरिंग के लिए नेटफ़िल्टर फ्रेमवर्क को सक्षम करना है।

5.1 नेटवर्क ब्रिज स्थापित करना

लिनक्स आधारित नेटवर्क ब्रिज स्थापित करने के लिए सर्वप्रथम लिनक्स कर्नल में नेटवर्क ब्रिजिंग को सक्षम (इनेबल) करना पड़ता है | तदुपरांत आई पी लेयर और ईथरनेट (MAC) लेयर के बीच एक ब्रिज लेयर जोड़ना आवश्यक होता है | लिनक्स आधारित नेटवर्क ब्रिज स्थापित करने की बिधि को आगे समझाया गया है |

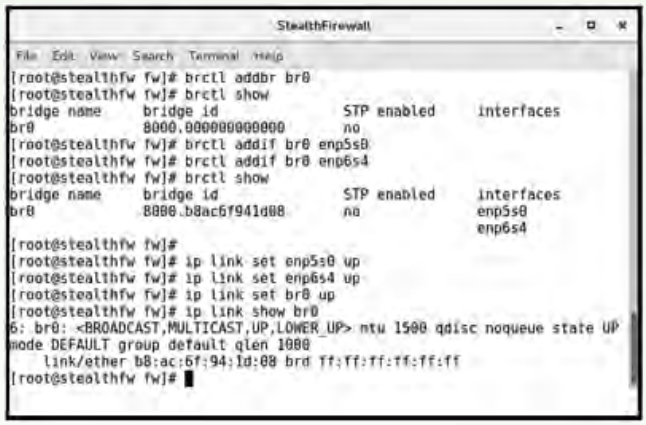
ब्रिजिंग कर्नल संस्करण 2.4 के बाद के सभी प्रमुख लिनक्स वितरणों में उपलब्ध रहती है। लिनक्स ओएस में ब्रिजिंग को "नेटवर्किंग सपोर्ट ->नेटवर्किंग आप्शन ->

802.1डी ईथरनेट ब्रिजिंग" को हां या मॉड्यूल पर सेट करके कर्नल विन्यास (कॉन्फ़िगरेशन) में सक्षम किया जा सकता है (जैसा कि चित्र-8 में दर्शाया गया है)। ब्रिज को विन्यासित (कॉन्फ़िगर) करने के लिए ब्रिज-यूटिल्स [19] पैकेज की आवश्यकता है। आधुनिक लिनक्स वितरण आमतौर पर इस पैकेज को डिफ़ॉल्ट रूप से उपलब्ध कराते हैं



चित्र-8, लिनक्स आधारित नेटवर्क ब्रिजिंग करने के लिए कर्नेल कॉन्फ़िगरेशन

ब्रिज को विन्यासित (कॉन्फ़िगर) करना ईथरनेट ब्रिज इंटरफ़ेस बनाने की नींव है; यह आई पी लेयर और ईथरनेट (MAC) लेयर के बीच एक ब्रिज लेयर जोड़ने के लिए आवश्यक है। लिनक्स आधारित नेटवर्क ब्रिज बनाने के लिए कमांड brctl addbr br0 का उपयोग किया जा सकता है जैसा कि चित्र 9 में दर्शाया गया है। यह कमांड ब्रिज br0 बनाता है। अब इस ब्रिज में उन नेटवर्क इंटरफेस को जोड़ना होता है, जिन्हें ब्रिज का हिस्सा बनना चाहिए। एक बार ब्रिज से जुड़ने के बाद, ये नेटवर्क इंटरफेस ब्रिज के पोर्ट बन जाते हैं| तदुपरांत नेटवर्क ब्रिज को सक्षम (इनेबल) करना होता है| यह ध्यान रखना महत्वपूर्ण है कि ब्रिज से जुड़े हुए नेटवर्क अंतराफलक (इंटरफ़ेस) eth0 और eth1 को IP एड्रेस नहीं देना चाहिए! आवस्यकता अनुसार आभासी (वर्चुअल) ब्रिज इंटरफ़ेस br0 एक आईपी एड्रेस का उपयोग कर सकता है। इसकी आवश्यकता केवल तभी होती है जब मशीन को दूर से संचालित किया जाना हो। हमारे कार्यान्वयन में, हमने अपने फ़ायरवॉल को वास्तविक अर्थों में गुप्त (स्टेल्थ) बनाने के लिए ब्रिज इंटरफ़ेस को आईपी एड्रेस नहीं सौंपा है, और बनाए गए ब्रिज के बारे में जानकारी चित्र 9 में दिखाई गई है।



चित्र-9, लिनक्स आधारित नेटवर्क ब्रिज को विन्यासित (कॉन्फ़िगर) करना

5.2 नेटवर्क ब्रिज के लिए नेटफ़िल्टर सक्षम करना

जैसा के इस पत्र में पहले व्यखायांतित किया गया है कि ब्रिज मोड में, ब्रिज किए गए नेटवर्क पैकेट पर केवल ईबीटेबल्स आधारित फ़िल्टरिंग क्षमता का ही उपयोग किया जा सकता है| क्योंकि ब्रिज किए गए पैकेट आईपीटेबल्स श्रृंखलाओं से नहीं गुजरते हैं [10]। ब्रिज किए गए पैकेटों पर आईपीटेबल्स आधारित फ़िल्टरिंग क्षमताओं का उपयोग करने के लिए, इन पैकेटों को आईपीटेबल्स श्रृंखलाओं (चेन्स) से गुजरना अवश्यक होता है| इस क्षमता को बनाने के लिए हमने लिनक्स कर्नेल मॉड्यूल (ब्रिज-एनएफ इंफ्रास्ट्रक्चर) का निर्माण किया | यह मॉड्यूल ब्रिज हुए लेयर-२ नेटवर्क पैकेट्स तो लेयर-3 (नेटवर्क लेयर) मैं पहुचता है और प्रोसेसिंग हो जाने का बाद पुनः लेयर-2 मैं बापस लता है, जैसा की चित्र-10 मैं दर्शाया गया है| यह कर्नल मॉड्यूल 50,000,00 पैकेट्स \सेकंड परसंस्करित (प्रोसेसिंग) करने मैं सक्षम है|

चित्र-10, ब्रिज-एनएफ इंफ्रास्ट्रक्चर लिनक्स कर्नेल मॉड्यूल

लिनक्स कर्नेल बूट समय पर इस मॉड्यूल को स्वचालित रूप से लोड नहीं करते हैं। इस मॉड्यूल को कर्नेल में लोड करने के लिए modprobe <मोड्यूल_नाम> चलाना आवश्यक है| Modprobe कमांड मॉड्यूल को लोड करता है लेकिन अगले बूट स्वतः लोड नहीं होता

है और प्रत्येक बूट पर लोडिंग की आवश्यकता होगी। सिस्टमड-मॉड्यूल-लोड.सर्विस (systemd-modules-load.service) डेमन बूट समय पर मॉड्यूल की स्वचालित लोडिंग की सुविधा प्रदान करता है [20]। इस मॉड्यूल की स्वचालित लोडिंग के लिए, /etc/modules-load.d/ डायरेक्टरी मैं एक फ़ाइल बनानी हिती है और इस फिने मैं में मॉड्यूल के नाम लिखना होता है।

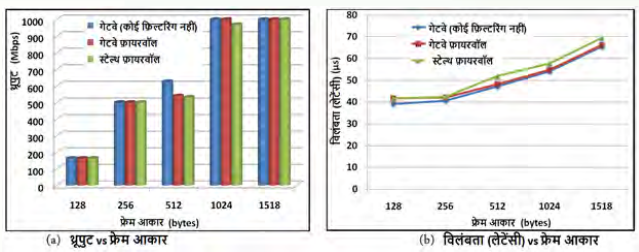
एक बार ब्रिज कॉन्फ़िगर हो जाने के बाद, नेटफिल्टर सक्षम (इनेबल) हो जाता है और पैकेट ब्रिज मॉड्यूल कर्नेल में लोड हो जाता है| इसके साथ ही यह उपकरण एक स्टेल्थ फ़ायरवॉल के रूप में काम करने के लिए तैयार हो जाता है। पारंपरिक लेयर-3 पैकेट फ़िल्टरिंग फ़ायरवॉल की तरह, यह स्टेल्थ फ़ायरवॉल फ़िल्टरिंग नीति को लागू करने के लिए आईपीटेबल्स रूल्स सेट का उपयोग कर सकता है। यह स्टेल्थ फ़ायरवॉल ईबटेबल्स का उपयोग करके लेयर-2 ट्रैफ़िक को भी फ़िल्टर कर सकता है, जो पारंपरिक गेटवे फ़ायरवॉल की तुलना में एक अतिरिक्त क्षमता है।

6 निष्पादन मूल्यांकन हेतु प्रयोग और परिणाम

हमने अपने स्टेल्थ फ़ायरवॉल के निष्पादन मूल्यांकन (परफॉरमेंस इवैल्यूएशन) हेतु उपलब्ध मानको के अनुसार कई प्रयोग किये, इनका विवरण इस अनुभाग में प्रस्तुत किया गया है| हमने तुलनात्मक निष्पादन मूल्यांकन के लिए नेटवर्क उपकरण जैसे की गेटवे (कोई फ़िल्टरिंग नहीं), गेटवे फ़ायरवॉल और स्टेल्थ फ़ायरवॉल रूप में थ्रूपुट और विलंबता को मापने के लिए प्रयोग किए। हमने इस मापन के लिए स्पाईरेंट टेस्टसेंटर SPT-2000A और एक होस्ट मशीन जिसमें 8 जीबी रैम, दो-गीगाबिट ईथरनेट एडेप्टर के साथ 2.93 गीगाहर्ट्ज पर संचालित इंटेल i7 सीपीयू उपस्तिथ है के उपयोग किया । प्रयोगात्मक स्थापना चित्र 11 में दर्शया गया है।

चित्र-11, निष्पादन मूल्यांकन (परफॉरमेंस इवैल्यूएशन) के लिए प्रयोगात्मक स्थापना

गेटवे रूप (कोई फ़िल्टरिंग नहीं) में, होस्ट को केवल आईपी ट्रैफ़िक को अग्रेषित (फॉरवर्ड) करने के लिए कॉन्फ़िगर किया गया। गेटवे फ़ायरवॉल रूप में, होस्ट को प्रोटोकॉल, स्रोत आईपी, स्रोत पोर्ट, गंतव्य आईपी और गंतव्य पोर्ट के आधार पर आईपी ट्रैफ़िक को फ़िल्टर करने के लिए कॉन्फ़िगर किया गया। स्टेल्थ फ़ायरवॉल रूप में, होस्ट को ब्रिज के रूप में कॉन्फ़िगर किया गया है और इस मोड के लिए समान फ़िल्टरिंग नियम विन्यासित (कॉन्फ़िगर) किए गए। नेटवर्क थ्रूपुट और विलंबता को मापने के लिए RFC 2544 [21] और RFC 2679 [22] में उल्लिखित मानकों का उपयोग किया | इन मानकों के अनुसार 128 से 1518 बाइट्स तक के विभिन्न फ्रेम आकारों के लिए थ्रूपुट और विलंबता (लेटेंसी) को मापा जाता है।



चित्र-12, प्रयोग परिणाम

प्रयोग के परिणाम चित्र 12 में दर्शाए गए हैं। स्टेल्थ फ़ायरवॉल मोड के लिए नेटवर्क थ्रूपुट गेटवे मोड (कोई फ़िल्टरिंग नहीं) की तुलना में थोड़ा कम है और औसत विलंबता थोड़ी अधिक है, लेकिन वे पारंपरिक गेटवे फ़ायरवॉल मोड के लगभग समान हैं।

7 निष्कर्ष

नेटवर्क सुरक्षा में, फ़ायरवॉल का बहुत महत्वपूर्ण स्थान होता है और किसी भी नेटवर्क में संपूर्ण सुरक्षा नीति (सिक्यूरिटी पालिसी)को लागू करने के लिए फ़ायरवॉल पर भरोसा किया जाता है। नेटवर्क सुरक्षा मैं फ़ायरवॉल रक्षा की पहली पंक्ति होती है, जिसे नेटवर्क की सुरक्षा के लिए पूरक नेटवर्क सुरक्षा समाधानों के साथ तैनात (डेपलॉय) किया जाता है। फ़ायरवॉल विश्वसनीय और अविश्वसनीय नेटवर्क के बीच एक मजबूत परिधि रक्षा का गठन करके उद्यम (एंटरप्राइज) नेटवर्क सुरक्षा की नींव बन जाता है। फ़ायरवॉल को हराने का एक तरीका इसे सीधे लक्षित (टारगेट) करना है। पारंपरिक लेयर-3 पैकेट फ़िल्टरिंग फ़ायरवॉल को आमतौर पर गेटवे या राउटर के रूप में कार्यान्वित किया जाता है और इसमें आईपी एड्रेस होते हैं। पारंपरिक पैकेट फ़िल्टर फ़ायरवॉल की यह आईपी दृश्यता (विजिबिलिटी) विशेषता उन्हें नेटवर्क हमलों के प्रति संवेदनशील बनाती है। इस भेद्यता को दूर करने के लिए, हम OSI मॉडल में

एक लेयर नीचे आकर यानी कि लेयर-2 पर फ़ायरवॉल की कल्पना की। हमारा यह दृष्टिकोण फ़ायरवॉल को आंतरिक और बाहरी दोनों नेटवर्क से अदृश्य बनाकर गुप्त (स्टैल्थ) बना देता है।इस स्टैल्थ फ़ायरवॉल को अपने स्वयं के लिए किसी आईपी एड्रेस की आवश्यकता नहीं पड़ती है और इसलिए यह आईपी का उपयोग करने वाले किसी भी हमले से प्रतिरक्षित (इम्यून) हो जाती है। स्टैल्थ फ़ायरवॉल का निर्माण करने में, हमने लिनक्स के नेटफिल्टर फ्रेमवर्क, ब्रिजिंग, आईपीटेबल्स और आईपीटेबल्स क्षमताओं का लाभ उठाया।आईपीटेबल्स और आईपीटेबल्स का संयोजन इस स्टैल्थ फ़ायरवॉल को एक शक्तिशाली फ़िल्टरिंग उपकरण बना देता है।इस फ़ायरवॉल में पारंपरिक लेयर-3 लिनक्स पैकेट फ़िल्टरिंग फ़ायरवॉल की सभी क्षमताएँ के साथ-साथ लेयर-2 पर नेटवर्क ट्रैफ़िक फ़िल्टर करने की अतिरिक्त क्षमता भी उपलब्ध है।स्टैल्थ फ़ायरवॉल से किसी भी मौजूदा नेटवर्क में निर्बाध तैनाती का लाभ भी मिलता है और नेटवर्क प्रशासक को नेटवर्क रीडिज़ाइन और नेटवर्क उपकरणों के आईपी विन्यास (कॉन्फ़िगरेशन) परिवर्तनों के दर्द से राहत मिल जाती है। गोपनीयता, शून्य नेटवर्क परिवर्तन और तेजी से तैनाती , हमारी इस स्टैल्थ फ़ायरवॉल को पारंपरिक लेयर -3 लिनक्स पैकेट फ़िल्टरिंग फ़ायरवॉल का एक सार्थक विकल्प बनाती है।

संदर्भ:

1. Cheswick WR, Bellovin S, Rubin A (2003) Firewalls and internet security, 2nd edn. Addison-Wesley
2. Ranum MJ (1992) A network firewall. In: World conference on system administration and security, Washington. DC, pp 153–163
3. Chapman D, Zwicky E, Cooper S (2000) Building internet firewalls, 2nd edn. O'Reilly
4. Mogul J, Rashid R, Accetta M (1987) The packet filter: an efficient mechanism for user-level network code. In: Eleventh ACM symposium on operating systems principles, pp 39–51
5. Andreasson O (2006) IPtables tutorial 1.2.2
6. Chen S, Iyer R, Whisnant K (2002) Evaluating the security threat of firewall data corruption caused by instruction transient errors. In: International conference on dependable systems & network, Washington, DC, pp 495–504. 10.1109/DSN.2002.1028938
7. Ingham K, Forrest S (2002) A history and survey of network firewalls. ACM J 1–42 8. Benvenuti C (2009) Understanding linux network internals. O'Reilly Media
8. Russell R, Welte H (2002) Linux Netfilter Hacking HOWTO. Revesion 1:14
9. Ebtables and bridge. http://ebtables.netfilter.org. Last accessed 21 Apr 2019
10. Jianbing L, Yan M (1999) Packet filtering in bridge. In: Internet workshop. IEEEcommunications
11. society, Piscataway, NJ, pp 94–98
12. Keromytis AD, Wright JL (2000) Transparent network security policy enforcement. In: USENIX technical conference, San Diego, CA, pp 215–226
13. Rosen R (2013) Linux Kernel networking: implementation and theory. Apress
14. Gregor NP (2004) Linux Iptables pocket reference. O'Reilly Media
15. Tzu S (2019) The art ofwar. http://www.ccs.neu.edu/home/thigpen/html/art_of_war.html.
16. Ethernet Bridging. https://www.kernel.org/doc/html/latest/networking/bridge.html.
17. 802.1D MAC bridges IEEE standard. http://www.ieee802.org/1/pages/802.1D.html.
18. Ebtables patch download. ftp://ftp.netfilter.org/pub/ebtables/old/ebtables-brnf-13_vs_2.4.37.9.diff.gz.
19. Bridge-utils-1.6. http://www.linuxfromscratch.org/blfs/view/svn/basicnet/bridge-utils. html. Last accessed 21 Apr 2019
20. RHEL 7, Kernel Administration Guide. https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/kernel_administration_guide/index, 2018.
21. Bradner S, McQuaid J (2005) Benchmarking methodology for network interconnect devices. In: RFC 2544
22. Almes G, Kalidindi S, Zekauskas M (1999) A one-way delay metric for IPPM. In: RFC 2679

वितरित प्रणालियों में वर्टिकल और हॉरिज़ॉन्टल स्केलिंग की समझ

सुश्री आरती गुप्ता, व.त.स. 'बी'

परिचय

डिजिटल प्लेटफ़ॉर्मों के तेजी से बदलते परिदृश्य में, स्केलिबिलिटी और विश्वसनीय प्रणालियों की मांग दिन-प्रतिदिन बढ़ती जा रही है। वितरित प्रणालियों डेटा और उपयोगकर्ता भार का प्रबंधन करके इस मांग को पूरा करने में महत्वपूर्ण भूमिका निभाती हैं। स्केलिबिलिटी की दुनिया में हॉरिज़ॉन्टल स्केलिंग ओट वर्टिकल स्केलिंग दो महत्वपूर्ण अवधारणाएँ हैं। ये रणनीतियाँ प्रणालियों को विकास की स्थितियों को समर्थन देने और विभिन्न भार के तहत प्रदर्शन को बनाए रखने में सहायक होती हैं। इस लेख में, हम हॉरिज़ॉन्टल और वर्टिकल स्केलिंग की जटिलताओं, उनके महत्व, अनुप्रयोगों और विभिन्नताओं का अन्वेषण करते हैं।

वर्टिकल स्केलिंग: स्केलिंग अप

वर्टिकल स्केलिंग, वर्तमान अवसंरचना के भीतर एक एकल मशीन या नोड के संसाधनों का उन्नतिकरण करना शामिल होता है। यह आमतौर पर मशीन की प्रोसेसिंग शक्ति, मेमोटी या स्टोरेज क्षमता को बढ़ाने की प्रक्रिया है। वऊध्वधिर स्केलिंग उन अनुप्रयोगों के लिए आदर्श है जिन्हें उच्च कम्प्यूटेशनल शक्ति या मेमोरी एक्सेस की आवश्यकता होती है। इसके अतिरिक्त, वर्टिकल स्केलिंग सर्वट को पूरी तरह से बदलने या सर्वेट के कार्यक्षमता को एक उन्नत मशीन पर स्थानांतरित करने का वर्णन भी करती है।

वर्टिकल स्केलिंग के लाभ:

1. सरलता एकल मशीन को उन्नतिकरण करना अक्सर कई मशीनों को हॉरिज़ॉन्टली स्थायीकृत करने से संचालन में अधिक सटल होता है।
2. इंटरप्रोसेस संचार: एक ही नोड के भीतर चल रहे प्रक्रियाओं के चीच संचार मशीनों के बीच नेटवर्क संचार से तेज़ होता है। एप्लिकेशन्स और सेवाओं के बीच संचार पथ छोटा होता है, क्योंकि समक्रमण और अनुरोधों की जानकारी लगभग तुरंत होती है, क्योंकि किसी बाधिक प्रविष्टि की आवश्यकता नहीं होती है।
3. डेटा कंसिस्टेंसी: वर्टिकल स्केलिंग का एक और महत्वपूर्ण लाभ यह है कि डेटा एक ही मशीन पर रहता है। एकल मशीन होने के कारण, नोड़ों के बीच समक्रमण और डेटा कंसिस्टेंसी की चिंता करने की कोई आवश्यकता नहीं होती है, जो हॉरिजॉन्टल स्केलिंग के साथ संभव नहीं होता है। डेटा कंसिस्टेंसी विशेष रूप से उच्च-संगणकता अनुप्रयोगों के लिए महत्वपूर्ण है जो तेज़ संचार पर निर्भर होते हैं और ऐसे अनुप्रयोगों के लिए जिन्हें तुरंत लिंक किया जाना चाहिए।

वर्टिकल स्केलिंग के दुष्प्रभाव

1. विफलता का एकल बिंदुः एकल सर्वर पर चलने वाले एप्लिकेशन का मुख्य नुकसान यह है कि यह विफलता के एकल बिंदु का प्रतिनिधित्व करता है। यदि, किसी कारण से, मशीन विफल हो जाती है, तो आपका आवेदन भी विफल हो जाता है। हार्डवेयर की खराबी, करप्ट सॉफ्टवेयर, मैलवेयर या अन्य प्रकार के कुख्यात लक्षित हमले, या डेटा सेंटर में व्यावसायिक दुर्घटनाएँ, महंगी डाउनटाइम की ओर ले जा सकती हैं, जिन्हें हॉरिज़ॉन्टल स्केलिंग से ठीक किया जा सकता है।
2. डाउनटाइम में वृद्धिः वर्टिकल स्केलिग में, हमें हार्डवेयर को बदलने या अपग्रेड करने की आवश्यकता होती है इसलिए इसके परिणामस्वरूप डाउनटाइम में वृद्धि होगी। प्रावधान के दौरान, हार्डवेयर जोड़ने के लिए सर्वर को बंद करने की आवश्यकता हो सकती है। यदि डिस्क स्थान बढ़ता है, तो एक औट ड्राइव जोड़ने की आवश्यकता हो सकती है। इस प्रकार, यह भी एक संभावना है कि डिस्क सिंक्रोनाइजेशन के कारण सर्वर पूरी तरह से संचालन क्षमता पर पहुंचने तक अतिरिक्त डाउनटाइम ले सकता है।
3. हार्डवेयर और सॉफ़्टवेयर की सीमाएँ: एक एकल मशीन में कितना हार्डवेयर जोड़ा जा सकता है, इसकी एक सीमा है। लागत प्रदर्शन के मामले में एक निश्चित सीमा तक पहुंचना अधिक महंगा

हो जाता है। लेकिन इसके अतिरिक्त, हार्डवेयर और सॉफ्टवेयर सीमाएं भी हैं। उदाहरण के लिए, यदि आपके सॉफ्टवेयर का हिस्सा समानांतर में निष्पादित नहीं किया जा सकता है, तो हार्डवेयर जोड़ने से निष्पादन समय में सुधार नहीं होगा।

हॉरिज़ॉन्टल स्केलिंग: स्केलिंग आउट

हॉरिज़ॉन्टल स्केलिंग (जिसे स्केलिंग आउट भी कहा जाता है) वर्तमान अवसंरचना में अतिरिक्त नोड या मशीनों को जोड़ने की एक प्रक्रिया है, ताकि बढ़ते हुए नेटवर्क ट्रैफिक के भार का वितरण किया जा सके। यदि आप किसी सर्वर पर एक एप्लिकेशन की होस्टिंग कर रहे हैं और पाते हैं कि वह यातायात को संभालने के लिए अब असमर्थ है, तो आप एक सर्वर जोड़कर इस समस्या का समाधान कर सकते है। उदाहरण के लिए, यह एक के बजाय कई कर्मचारियों के बीच कार्यभार को कम करने के समान है। यह दृष्टिकोण, मशीनों के बीच कार्यभार को विभाजित करके, प्रणाली को यातायात और उपयोगकर्ता वृद्धि को संबोधित करने की क्षमता प्रदान करता है। प्रत्येक मशीन स्वतंत्र रूप से काम करती है, जिससे दोष सहिष्णुता और उपलब्धता में सुधार होती है। क्षैतिज स्थायीकरण विशेष रूप से ऐप्लिकेशन्स के लिए फायदेमंद है जो अचानक यातायात में वृद्धि या अपूर्व वृद्धि की पैटर्न का सामना करते हैं।

चित्र 1: वर्टिकल तथ हॉरिजॉन्टल स्केलिंग

हॉरिज़ॉन्टल स्केलिंग के लाभ:

1. बेहतर दोष प्रतिस्थानः अगर कोई मशीन असफल हो जाती है, तो भार स्वचालित रूप से अन्य मशीनों पर पुनर्निर्देशित होता है, हॉरिजॉन्टल स्केलिंग डाउनटाइम को कम करके सतत संचालन सुनिश्चित करती है।
2. स्केल करने में आसान: चूंकि आप अधिक मशीनों को स्थापित करके मौजूदा पूल में अधिक शक्ति जोड़ रहे हैं, इसलिए क्षैतिज स्केलिंग करते समय डाउनटाइम लगभग न के बटावर होता है। आपके द्वाटा जोडी जा सकने वाली मशीनों की संख्या की वस्तुतः कोई सीमा नहीं है। इसलिए, यह विकल्प आपके वर्तमान अवसंरचना के हार्डवेयर के आधार पर असीमित सैद्धांतिक विकास प्रदान करता है। संसाधनों को वास्तविक समय की मांग के आधार पर गतिशील रूप से जोड़ा या हटाया जा सकता है, तथा प्रणाली को लचीलापन और दक्षता प्रदान करता है।
3. बेहतर प्रदर्शनः एक साथ कई मशीनों के प्रसंटकटण अनुरोधों के साथ, सिस्टम तेजी से प्रतिक्रिया समय और बेहतर प्रदर्शन प्रदान कर सकता है।

हॉरिजॉन्टल स्केलिंग के नुकसान

1. रखरखाव और संचालन की बढ़ी हुई जटिलता एक सर्वर की तुलना में कई सर्वरों का रख-रखाव करना कठिन होता है। इसके अतिरिक्त, आपको लोड संतुलन और संभवतः वर्चुअलाइजेशन के लिए सॉफ्टवेयर की भी आवश्यकता होती है तथा मशीनों का बैकअप लेना भी अधिक जटिल हो सकता है। आपको यह सुनिश्चित करने की आवश्यकता होगी कि नोड्स सिंक्रनाइज़ और प्रभावी ढंग से संवाद करें।
2. बढ़ी हुई प्रारंभिक लागत नए सर्वट जोड़ना पुटाने के उन्नत करने की तुलना में कई गुना महंगा होता है।

सही रणनीति का चयन

हॉरिज़ॉन्टल और वर्टिकल स्केलिंग दोनों ही अपने लाभ और सीमाएँ रखते हैं। आपको अपनी आवश्यकताओं और संसाधनों के अनुसार स्केल कटने की आवश्यकता है। एप्लीकेशन के लिए स्केलिंग का चायत करते समय आपको निम्नलिखित बिंदुओं को ध्यान में रखना चाहिए। एप्लीकेशन के लिए स्केलिंग का चायत करते समय आपको निम्नलिखित बिंदुओं को ध्यान में रखना चाहिए।

1. लागतः हॉरिज़ॉन्टल उन्नतियों के लिए प्रारंभिक हार्डवेयर लागतें अधिक होती हैं। यदि आप कम

बजट पर काम कर रहे हैं और अपने अवसंरचना में शीघ्र और सस्ते तरीके से ओट संसाधनों को जोड़ने की आवश्यकता है, तो वर्टिकल स्केलिग आपके लिए सबसे अच्छा विकल्प हो सकता है।

2. भविष्य-सुरक्षितः हॉरिज़ॉन्टल स्केलिंग के माध्यम से अतिरिक्त अद्यतित मशीनों को जोड़ने से आपके संगठन के कुल प्रदर्शन सीमा बढ़ जाएगी तथा आप भविष्य में बढ़ती हुई मांगों को सफलतापूर्वक पूरा कर पाएंगे। एकल नोड को वर्टिकल स्केल करने की एक निर्धारित सीमा होती है और यह भविष्य की बढ़ती हुई मांगों का सामना करने में असमर्थ हो सकता है।

3. भूगोलिक वितरणः यदि आपके पास राष्ट्रीय या वैश्विक ग्राहक होने की योजना है. तो उम्मीद करना गलत है कि वे सभी एक ही स्थान में एक ही मशीन से आपकी सेवाओं का उपयोग करेंगे। इस तरह की स्थिति में, आपको अपने सेवा स्तर समझौते को बनाए रखने के लिए अपने संसाधनों को हॉरिजॉन्टल स्केल करने की आवश्यकता होगी।

4. विश्वसनीयताः हॉरिज़ॉन्टल स्केलिंग आपको एक अधिक विश्वसनीय प्रणाली प्रदान कर सकती है। यह पुनरावृत्ति को बढ़ाता है और सुनिश्चित करता है कि आप केवल एक मशीन पर निर्भट नहीं हो रहे हैं। यदि कोई मशीन असफल होती है, तो दूसरी मशीन अस्थायी रूप से इसका संघटन कर सकती है।

5. प्रदर्शन और जटिलताः आपकी सेवाएं काम केसे करती हैं और वे केसे आपस में जुड़ी हैं, इस पर प्रदर्शन निर्भर करेगा। सरल सीधी एप्लिकेशने जब कई मशीनों पर चलती हैं, तब हॉरिजॉन्टल स्केलिंग उनकी गुणवत्ता को गिरा सकता है। कभी-कभी बेहतर होता है कि एप्लिकेशन के बढ़ते हुए नेटवर्क ट्रैफिक की मांग को पूरा करने के लिए हार्डवेयर को अपग्रेड करे अथर्थात वर्टिकल स्केलिंग का उपयोग करें। हॉरिज़ॉन्टल स्केलिंग में, आपको कोड को पुनलिखित करने तथा एक वर्चुअल मशीन, जो सभी सर्वरों को एकत्र करती है, जोड़ने की आवश्यकता हो सकती है।

निष्कर्ष

वितरित प्रणालियों के गतिशील परिदृश्य में, वर्टिकल और हॉरिज़ॉन्टल स्केलिंग को समझना उन प्रणालियों को डिजाइन करने के लिए महत्वपूर्ण है जो आधुनिक डिजिटल प्लेटफार्मों की मांगों को संभाल सकते हैं। दोनों रणनीतियों अद्वितीय लाभ प्रदान करती हैं जो उन्हें मापनीयता, दोष सहिष्णुता और प्रदर्शन अनुकूलन प्राप्त करने के लिए शक्तिशाली उपकरण बनाती हैं। एप्लिकेशन की जरूरतों और इसकी अनुमानित वृद्धि का सावधानीपूर्वक आकलन करके, डेवलपर्स इस बारे में सूचित निर्णय ले सकते हैं कि कौन सी स्केलिंग रणनीति, या उसका संयोजन, उनकी विशिष्ट आवश्यकताओं के लिए सबसे उपयुक्त है।

संदर्भ:

1. Horizontal vs Vertical Scaling: Which One Is Best For You? | Liquid Wich
2. Horizontal Vs. Vertical Scaling: How Do They Compare? (cloudzero.com)
3. Overview of Scaling: Vertical And Horizontal Scaling - GeeksforGeeks
4. A Guide To Horizontal Vs Vertical Scaling MongoDB

लेखक परिचय:

कुमारी आरती गुप्ता ने कंप्यूटर साइंस में स्नातकोत्तर की उपाधि प्राप्त की है तथा वर्तमान में कृत्रिम ज्ञान तथा रोबोटिकी केंद्र, बेंगलुरु में वरिष्ठ तकनीकी सहायक बी' के पद पर कार्यरत है।

कृत्रिम ज्ञान तथा रोबोटिकी केन्द्र: दृष्टि

सूचना संवर्धन द्वारा रणक्षेत्र प्रभुत्व हेतु सामर्थ्य विकास

कृत्रिम ज्ञान तथा रोबोटिकी केन्द्र: लक्ष्य

सूचना संवर्धन के लिए ऐसी विश्वसनीय प्रौद्योगिकी एवं प्रणालियों को विकसित करना, जो रक्षा सेवाओं के रणक्षेत्र प्रभुत्व हेतु संरक्षा, सुरक्षा, नम्यता, उत्तरजीविता तथा विश्वस्तता सुनिश्चित करे तथा अति महत्वपूर्ण अनुप्रयोगों के आश्वासित निष्पादन को विश्वसनीय बनाएं।

हम इसे निम्न द्वारा प्राप्त करते हैं

रणक्षेत्र सूचना प्रणाली प्रभाविता एवं दृढ़ता को सक्षम एवं प्रबल बनाने के लिए प्रौद्योगिकी को विकसित करना।

रणक्षेत्र की बाधित तथा प्रतिकूल परिस्थिति के लिए आश्वासित निष्पादन चुनौती के उपाय हेतु प्रणाली विकास।

उभरते साइबर सुरक्षा चुनौती को प्रत्याशित करना तथा उसे अग्रसक्रियता से सुलझाना।

मानवरहित प्रणाली में स्वायत्तता प्राप्त करने के लिए संज्ञानात्मक तथा कृत्रिम ज्ञान प्रणाली विकास कार्य को उद्यामन करना।

राष्ट्रीय सुरक्षा तथा आत्म-निर्भरता के संरक्षण के लिए महत्वपूर्ण प्रौद्योगिकी नीति के राष्ट्रीय तर्क को सुनियोजित करना।

हमारे सिद्धांत

केवल व्यवसायी व्यवहार से नहीं बल्कि विचारपूर्ण नम्यता। नए विचारों को स्वीकार करना तथा अपनाना एवं विफलता से सीखना।

केवल सुरक्षा नहीं बल्कि सुविचारित जोखिम। विफलता विनाशकारी नहीं होती क्योंकि यह अन्वेषण क्षेत्र के दायरे को कम करते हुए सार्थक अनुकूलन का मार्ग प्रशस्त करती है।

केवल लक्ष्य पर नहीं बल्कि प्रक्रिया पर ध्यान केंद्रित करना। यदि हम ठीक से कार्य करें, तो हम लक्ष्य तक पहुँच सकते हैं। क्षमता में निरंतर सुधार द्वारा लक्ष्य को प्राप्त करने का प्रयत्न करना।

अनुशासित वर्गीकरण नहीं बल्कि सम्मिलित कार्य सभ्यता। विचारों के मतभेद, प्रौद्योगिकी विप्लव, विशिष्ट विचार को प्रोत्साहित करना।

केवल विशेषज्ञ को नहीं बल्कि प्रयोक्ता को सुनना। भले ही विशेषज्ञों द्वारा प्रौद्योगिकी विकसित होती है परंतु इसका प्रयोग प्रयोक्ता करता है। हमें प्रयोक्ता को संतुष्ट करना है न कि स्वयं को।

सर्वप्रथम सत्यनिष्ठा तथा आचारनीति।

कृत्रिम ज्ञान तथा रोबोटिकी केन्द्र

रक्षा अनुसंधान एवं विकास संगठन

रक्षा मंत्रालय, भारत सरकार

सी.वी. रामन नगर, बेंगलूरु - 560 093, भारत