संस्थांत होणाऱ्या तिरकस लक्ष्यित सोंगजाळ्यांचा शोध

अनिकेत भदाने

संस्थात्मक क्रमांक : १२१६२२००१

यांजकडून

डॉ. सुनील भ. माने

यांच्या मार्गदर्शनाखाली

संगणक अभियांत्रिकीत स्नातकोत्तर

पदवी प्रदानाच्या आंशिक पूर्ततेसाठी

हा प्रबंध

शासकीय अभियांत्रिकी महाविद्यालय, पुणे (सी.ओ.ई.पी.)

संगणक अभियांत्रिकी व माहिती तंत्रज्ञान विभाग,

शासकीय अभियांत्रिकी महाविद्यालय (सी.ओ.ई.पी.), पुणे - ५

मे, २०१८

ऋणनिर्देश

माइया प्रबंधाचे मार्गदर्शक डॉ. सुनील भ. माने यांना या संपूर्ण प्रवासादरम्यान आपल्या सातत्याच्या पाठिंब्यासाठी मी माझी प्रामाणिक आणि मनापासून कृतज्ञता व्यक्त करू इच्छितो. ज्या सर्व स्वैच्छिकांनी माहितीसंग्रह बनवण्यासाठी आपला विपत्रांचा इतिहास सामायिक केला, त्याबद्दल मी कृतज्ञ आहे ज्याशिवाय ह्या संशोधनाला मोठा अडथळा आला असता. जेव्हा गरज असेल तेव्हा मला आवश्यक मदत पुरविण्यासाठी मी संगणक अभियांत्रिकी आणि माहिती तंत्रज्ञान विभाग आणि हेल्पडेस्क गटाच्या सर्व अध्यापक सदस्यांना धन्यवाद देतो. मी माइया सहकार्यांबद्दल कृतज्ञता व्यक्त करतो ज्यांच्याशी मी या प्रकल्पावर मौल्यवान चर्चा केली. अंततः, परंतु महत्त्वाचे म्हणजे, माइया पालकांचे, ज्यांनी माइयावर नेहमीच निरपेक्ष प्रेम केले आहे.

सारांश

सामाजिक अभियांत्रिकीचे सहाय्य घेऊन हल्लेखोर हे लोकांची मानसिक हेरफेर करून त्यांना हल्लेखोरांच्या फायद्यासाठी काही कृती करण्यास प्रवृत्त करतात. सोंगजाळ्यांचे हल्ले विश्वासार्ह स्त्रोत असल्याचे सोंग करतात, आणि विपत्रे, समाज माध्यमे, लघू संदेश, महाजालावरील सांघिक खेळ, व्ही-ओआयपी इत्यादीसारख्या माध्यमांद्वारे सामाजिक अभियांत्रिकी वापरून बनवलेल्या संदेशांद्वारे पसरतात. सामाजिक अभियांत्रिकी वापरून बनवलेलले संदेश वापरकर्त्यांना घातक/सोंगजाळी दुव्यांवर टिचकी मारणे ; सोंगजाळी संकेतस्थळावर वापरकर्त्यासंबंधी संवेदनशील माहिती प्रविष्ट करणे ; कृती जसे पैसे हस्तांतरण करणे, घातक संगणक कार्यक्रम स्थापित करणे इत्यादी, ह्यासारख्या गोष्टी करण्यास प्रवृत्त करतात. सोंगजाळे हे संस्थांचे आणि व्यक्तींचे मूर्त आणि अमूर्त नुकसान करून मोठी समस्या ठरतच आहेत.

तिरकस लक्ष्यित सोंगजाळ्यांचे हल्ले हे सामाजिक अभियांत्रिकी हल्ल्यांचा एक शक्तिशाली वर्ग आहे जे हल्लेखोरांच्या ताब्यात असलेल्या लक्ष्यित संस्थेतल्या एक किंवा अनेक खात्यांतून केले जातात. लक्ष्यित सोंगजाळी हल्ले त्यांच्या स्वरूपामुळे शोधणे कठिण आहेत. त्यात तिरकस प्रकार समाविष्ट झाल्याने अशे हल्ले शोधणे अधिक आव्हानात्मक आहे. आम्ही वास्तविक-वेळेमध्ये संस्थांमध्ये होणाऱ्या तिरकस लक्ष्यित सोंगजाळ्यांना शोधण्यासाठी एक पद्धत सादर करतो. आम्ही आमच्या पद्धतीत क्षेत्रासंबंधी ज्ञान आणि अशा प्रकारच्या हल्ल्यांचे विश्लेषण करून प्राप्त केलेले वैशिष्ट्ये, आमच्या मुल्यांकन प्रणाली सोबत वापरतो जी खूणचिट्ठी नसलेल्या माहितीसंग्रहावर काम करते. आमच्या संस्थेतील स्वैच्छिकांकडून स्वयंसेवकांकडून एकत्रित केलेल्या वास्तविक जीवनातील माहितीसंग्रहाचा वापर करून आम्ही आमच्या पद्धतीचे मूल्यांकन करतो. आम्ही १% च्या खाली `चुकीचे-सकारात्मक' दर प्राप्त केले व आम्हाला पूर्वी अज्ञात असलेलले २ हल्ल्यांचे प्रसंग देखील सापडले. यंत्र स्वशिक्षण तंत्रज्ञानावर आधारीत विसंगती शोध पद्धतींसोबत तुलना केल्यास, आमची मुल्यांकन प्रणाली व्यवहार्य वापरासाठी अधिक उपयुक्त असल्याचे दिसते. प्रस्तावित पद्धत पध्दत प्रामुख्याने विपत्र प्रसंगणकांवर विद्यमान शोध तंत्रांना पूरक आहे. परंतु, अशी प्रणाली संस्था स्वतंत्ररीत्या देखील वापरू शकतात हे प्रदर्शित करण्यासाठी आम्ही एक ख्रोम एक्सटेन्शन देखील विकसित केले आहे.

अनुक्रमणिका

कोष्टकांची यादी

आकृत्यांची यादी

प्रकरण १

भूमिका

सोंगजाळ्यांचा हल्ला शब्दार्थासंबंधीचा हल्ला आहे. हे हल्ले प्रणालींवर प्रदर्शित झालेल्या मजकूराचे विश्लेषण करण्याच्या मानवी भेद्यतेला लक्ष्यित करून त्याचा गैरफायदा घेतात. हे सामान्यतः सामाजिक अभियांत्रिकी वापरून केले जाते. सोंगजाळ्यांच्या हल्ल्यात तीन प्रमुख टप्पे असतात : पहिला टप्पा हा आमिषाशी निगडीत असतो. यात लक्ष्यितांना सामाजिक अभियांत्रिकी वापरून बनवलेले संदेश पाठवले जातात ज्यात प्रेषक एका विश्वसनीय ओळख असल्याचे सोंग करत असतो. दुसरा आणि तिसरा टप्पा हे गैरफायद्याशी निगडीत आहेत, जिथे लक्ष्यित माणूस संदेशात सुचविल्याप्रमाणे कृती करतो आणि हल्लेखोर स्वतःच्या फायद्यासाठी लक्ष्यिताने केलेल्या कृतीचा गैरवापर करतो.

लक्ष्यित सोंगजाळ्यांचे हल्ले संस्थांचे आणि व्यक्तींचे प्रचंड मूर्त आणि अमूर्त नुकसाण करत असल्यामुळे आंतरजालीय हल्ल्यांच्या प्रकाशझोतात आहेत [२७]. व्हॉनाक्राय रॅनसमवेअर हल्ल्याच्या सहभागिता प्रसिध्द लझारूस गटाने अलीकडे एक लक्ष्यित सोंगजाळी मोहिम सुरु केली ज्यात ते एका क्रिप्टोकरन्सी उद्योग संस्थेत सीएफओ ची रिक्त जागा भरण्यात येत आहे असे आमिष दाखवत होते [७१]. क्रिप्टोकरन्सींच्या किमतीत वाढ झाल्याने, २०१७ नंतर क्रिप्टो-सोंगजाळ्यांमध्येमध्ये मोठी वाढ झाली आहे [४७]. अमेरिकेतील फ्लोरिडाच्या एजन्सी फॉर हेल्थ केअर ऍडमिनिस्ट्रेशनचा एक कर्मचारी सोंगजाळी हल्ल्याला बळी पडल्याने ३०,००० मेडीकेड प्राप्तकर्त्यांची संवेदनशील माहिती गहाळ झाली. सर्व पारकरच्या संस्था, ते सरकारी असो किंवा खाजगी किंवा स्वयंसेवी, अशा प्रकारच्या हल्ल्यांना बळी पडले आहेत [२६]. अशे विपत्र वर्तमान घटनांचा देखील वापर करून लोकांना फसवण्याचा प्रयत्न करतात [४२].

लक्ष्यित सोंगजाळ्यांची विपत्रे ठराविक व्यक्ती किंवा संस्थांकडे लक्ष्यित केले जातात आणि हल्लेखोराचा फायदा होईल अशा कृती सामाजिक अभियांत्रिकी पद्धती वापरून लक्ष्यितांकडून करून घातल्या जातात. कृती ह्या विविध प्रकारच्या असू शकतात, जसे विपत्रातल्या दुव्यावर टिचकी मारणे आणि प-

रिणामी संकेतस्थळावर स्वतःची ओळखमाहिती लिहिणे ; किंवा स्वतःची अथवा संस्थेची संवेदनशील माहिती प्रदर्शीत करणे ; किंवा पैसे हस्तांतरण करणे, इत्यादी. लक्ष्यित सोंगजाळ्यांना सहाय्य करण्यासाठी अनेक संगणकीय साधनसंच उपलब्ध असल्यामुळे हल्लेखोर सहजपणे अशी मोहिम सुरु करू शकतात. सेवा-म्हणून-सोंगजाळे [३७] ने त्यांच्यासाठी हल्ले अधिक सोयीस्कर बनविले आहे. हल्ल्याची दृश्यमानता मर्यादित करून सोंगजाळी संकेतस्थळाचे जीवनमान वाढवण्यासाठी विविध पद्धतींचा वापर केला जातो [७२]. अशा हल्ल्यांपासून बचाव करणे कठिण असते कारण ते वैध वाटतील असे बनवले जातात. ७०% लक्ष्यित सोंगजाळ्यांची विपत्रे लक्ष्यितांकडून उघडले जातात आणि यापैकी ५०% वापरकर्ते विपत्रामधील दुव्यावर टिचकी मारतात [४८, २७].

तिरकस हल्ल्यामध्ये हल्लेखोर लक्ष्यित लक्ष्य संस्थेतले एक खाते ताब्यात घेतो, ज्यामुळे हल्लेखोराला संस्थेच्या आवारात एक पाया देतो. हल्लेखोर मग उच्च पातळीवरील कर्मचा-यांची ओळखमाहिती, आर्थिक माहिती, बौद्धिक मालमत्ता इत्यादी संवेदनशील माहिती लक्ष्यित करत तिरकस प्रकारे हालचाल करू शकतो. तिरकस लक्ष्यित सोंगजाळ्यांचा हल्ला हा आंतरजालीय हल्ल्यांचा एक शक्तिशाली वर्ग आहे ज्यामध्ये हल्लेखोराच्या ताब्यात असलेल्या संस्थेतल्याच खात्यातून संस्थेतल्या इतरांना लक्ष्यित सोंगजाळ्यांची विपत्रे पाठवली जातात. अशा प्रकारच्या हल्ल्या विशेषतः दुर्मिळ असतात परंतु ते संस्थांसाठी अत्यंत महाग पडू शकतात. अशा प्रकारचे हल्ले शोधण्याकरिता कोणतेही सर्वांगीण समाधान उपलब्ध नाही आणि सर्वोत्तम निकाल मिळविण्यासाठी त्यांचे क्षेत्रिय ज्ञानाचा समावेश करणे आवश्यक आहे [३५].

आम्ही शासकीय अभियांत्रिकी महाविद्यालय पुणे (सीओईपी, जी एक स्वायत्त अभियांत्रिकी संस्था आहे) ह्या संस्थेतल्या स्वैच्छिकांकडून विपत्रे गोळा केले. संस्थेत गेल्या काही वर्षात तिरकस लक्ष्यित सोंगजाळी हल्ले झाले आहेत. सीओईपी विपत्र सेवा प्रदाता म्हणून औद्योगिक आउटलुकचा वापर करते. सीओईपीत झालेले तिरकस लक्ष्यित सोंगजाळ्यांचे हल्ले प्रामुख्याने ओळखमाहिती मिळवणारे किंवा संवाद साधण्याचा प्रयत्न करणारे होते. माहितीसंग्रहामध्ये सर्व ज्ञात आक्रमण प्रसंग असतील ह्यासाठी आम्ही प्रयत्नशील होतो.

आमचा उद्देश एक व्यवहार्य आणि उपयोजनक्षम प्रणालीची मांडणी करणे आहे जी कमी चुकीचे- सकारात्मक दर ठेवत वास्तविक-वेळेमध्ये तिरकस लक्ष्यित सोंगजाळ्यांचे हल्ले शोधणे शक्य करते. मानक यंत्र स्वशिक्षण तंत्रज्ञानावर माहितीसंग्रहाच्या उच्च असंतुलनाचा परिणाम होतो आणि त्यांचा चुकीचे-सकारात्मक दर संस्थांमध्ये वापरासाठी अव्यवहार्य आहे. महत्त्वाचे म्हणजे, अंतर-क्षेत्रिय विपत्रे (प्रेषक आणि प्राप्तकर्ता त्याच संस्थेतले) बहुतांश वेळा गाळले जात नाहीत कारण त्यांचे `*विश्वासाचे*' गुण अधिक असतात [६८]. तिरकस लक्ष्यित सोंगजाळ्यांच्या विश्लेषणातून आम्ही वैशिष्ट्यांचा एक संक्षिप्त संच प्राप्त करतो. आमची मुल्यांकन प्रणाली संस्थेवर होणाऱ्या हल्ल्यांच्या क्षेत्रिय ज्ञानाचा उपयोग करून घेते. हे देखील असे सुचवते की प्रशासक आपल्या संस्थेशी संबंधित त्यांचे क्षेत्रिय ज्ञान

या प्रणालीमध्ये समाकलित करू शकतात. आम्ही आमच्या प्रणालीची तुलना यंत्र स्वशिक्षण तंत्रज्ञानावर आधारीत विसंगती शोध पद्धतींसोबत करतो आणि दाखवतो की आमची प्रणाली यंत्र स्वशिक्षण तंत्रापेक्षा चांगली अचूकता आणि चुकीचे-सकारात्मक दर देते.

आमची प्रणाली प्रामुख्याने विपत्र सेवा प्रदातांच्या प्रसंगणकांवर प्रस्थापित होऊन विद्यमान शोध तंत्रांना पूरक असे काम करेल. काही वाजवी कारणांमुळे हे शक्य नसल्यास, संस्था प्लगईन च्या सहाय्याने स्वतः अशा तंत्राची अंमलबजावणी करू शकते ज्यानेकरून विपत्रासंबंधित निर्णय घेण्यास वापरकर्त्यांना मदत होईल. आम्ही एक ख्रोम एक्सटेन्शन विकसित केले जे आमच्या मुल्यांकन प्रणालीचे आम्ही दिलेल्या एपीआय द्वारे सहाय्य घेत सीओईपीच्या वापरकर्त्यांना सीओईपीच्या आउटलुक खात्यावरील विपत्रांशी वागताना माहितीपूर्ण निर्णय घेण्यात मदत करतात. या कामाची मुख्य योगदाने आहेत :

- तिरकस लक्ष्यित सोंगजाळ्यांना शोधण्यासाठी वापरण्यायोग्य, वास्तविक-वेळेमध्ये काम करणारी प्रणाली.
- क्षेत्रिय ज्ञान आणि हल्ल्यांसंबंधीत खास वैशिष्ट्यांचा वापर, व खूणचिट्ठी नसलेल्या माहितीसंग्रहावर काम करणारी प्रणाली.
- अंतर-क्षेत्रिय विपत्रांचे अधिक विश्वासू गुण असेल्या आणि चुकीचे-सकारात्मक आणि चुकीचे-नकारात्मक कमी ठेवण्यासाठी आक्रमक नवगामी पद्धती वापरत नसलेल्या संस्थांमध्ये वापरण्यासाठी योग्य.
- प्रणाली जी प्रामुख्याने विपत्रांच्या प्रसंगणकांवर प्रस्थापित होऊन विद्यमान शोध तंत्रांना पूरक ठरेल. परंतु, संस्था जर प्रसंगणक व्यवस्थापित करत नसतील तर ते स्वतंत्ररीत्या सुद्धा अशी प्रणालीची अंमलबजावणी करू शकतात.

प्रकरण २ मध्ये आम्ही सोंगजाळ्यांवरील विद्यमान साहित्याबद्दलचे व आमच्या कामाशी संबंधित साहित्याबद्दलचे अवलोकन सादर करतो. आम्ही ह्या हल्ल्यांसंबंधित काही संकल्पना आणि आव्हाने प्रकरण ३ मध्ये सादर करतो. प्रकरण ४ मध्ये आम्ही गोळा केलेल्या माहितीसंग्रहाचे वर्णनात्मकरण सादर करतो. आम्ही वापरत असलेली वैशिष्ट्ये आणि आमच्या मुल्यांकन प्रणालीचे आम्ही प्रकरण ५ मध्ये वर्णन करतो. प्रकरण ६ मध्ये आम्ही आमच्या मुल्यांकन प्रणालीचे मूल्यमापन सादर करतो आणि त्याची कार्यक्षमता विसंगती शोध पद्धतींसोबत तुलना करतो. प्रकरण ७ मध्ये आम्ही ह्या काही चर्चा, प्रणालीच्या मर्यादा आणि आम्ही सीओईपी च्या वापरासाठी विकसित केलेल्या ख्रोम एक्सटेन्शन बद्दल काही तपशील प्रस्तुत करतो. प्रकरण ८ मध्ये आम्ही निष्कर्ष काढतो.

प्रकरण २

विद्यमान संशोधनाची स्थिती

२.१ सोंगजाळ्यांवरील साहित्याचा आढावा

झांग इ. [८१] ह्यांनी सोंगजाळ्यांविरोधातील कार्याचे चार वर्गात वर्गीकरण केले होते : लोक सोंगजाळ्यांना बळी का पडतात हे समजून घेणे, सोंगजाळे शोधण्यासाठी स्वयंचलित संगणक प्रणाली विकसित करणे, लोकांना सोंगजाळ्यांना बळी न पडण्याचे प्रशिक्षण देणे, लोकांना योग्य निर्णय घेण्यासाठी आंतरपृष्ठांद्वारे मदत करणे. परंतु, आम्ही असे मानतो की हे दोन मुख्य श्रेण्यांमध्ये सामान्यीकृत केले जाऊ शकतात : एक जे सोंगजाळ्यांतल्या मानवी मानसशास्त्राला समजून घेणे आणि दुसरे जे सोंगजाळ्यांपासून बचावासाठी तंत्रे विकसित करतात.

सोंगजाळी मानसशास्त्र

सोंगजाळी संदेश सामान्यतः भावना आणि मानसिक प्रभावाची तत्त्वे वापरतात, जसे प्राधिकरण, तुटवडा, कुतूहल, भीती, तात्कालिकता, सामाजिक पुरावे इत्यादी [७६]. [१८, ७९] ह्यांना असे आढळून आले की अगदी अनुभवी वापरकर्ते देखील दृष्टी फसवणुकीला बळी पडू शकतात. तसेच, [२१, २०] ह्यांनी दर्शविले की पारंपारिक जनजागृती पद्धतींची वापरकर्त्यांच्या हल्ल्यांसंबंधितची संवेदनशीलता कमी करण्यात फारशी मदत झाली नाही. कॅनफिल्ड इ. [९] ह्यांनी वापरकर्त्यांची ओळखण्याची - विपत्र सोंगजाळी आहे की नाही, आणि वर्तणूक - विपत्रासोबत कोणती क्रिया करावी हे ठरवणे, हे कार्यप्रदर्शन मापण्यासाठी प्रयोग केले. सिग्नल डिटेक्शन थिअरीच्या सहाय्याने ते दर्शवतात की वापरकर्त्यांचे सोंगजाळ्यांसंबंधित निर्णय हे त्यांच्या आत्मविश्वास आणि परिणामांबद्दलचे दृष्टिकोन या गोष्टींवर अवलंबून आहेत. तसेच, [७३] ह्यांनी दाखविले की, वापरकर्त्यांच्या वर्तणावर त्यांच्या स्वतःच्या

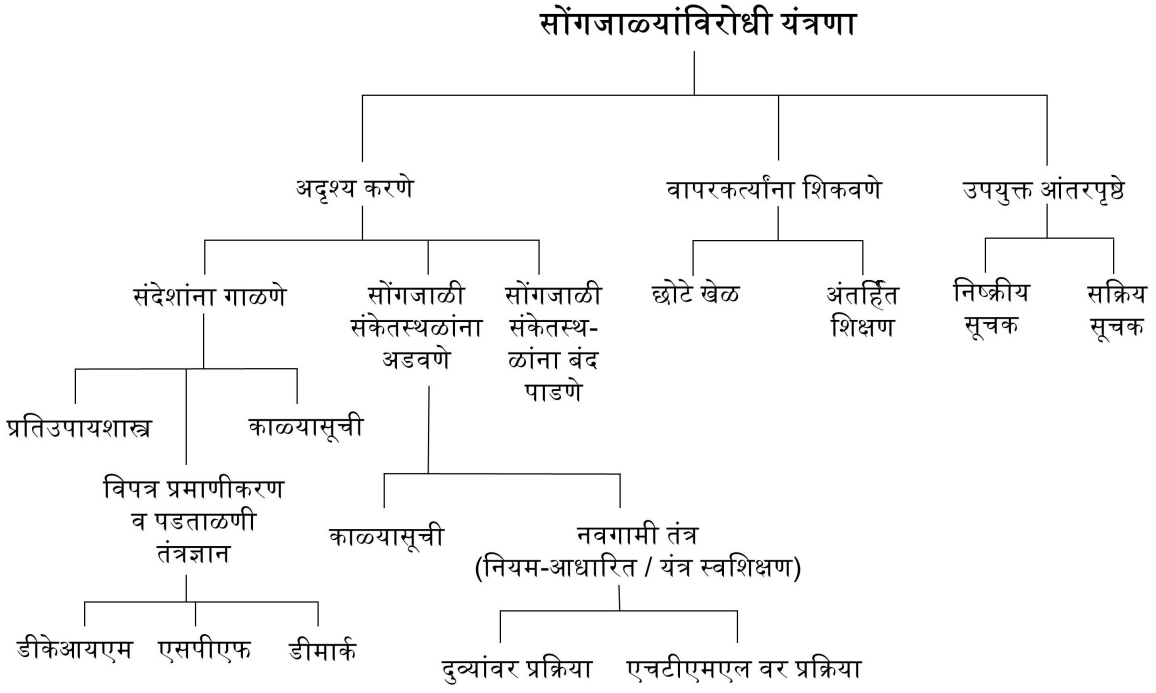
क्षमतेबद्दलच्या विश्वासापेक्षा अनुमानित आत्मविश्वासाचा अधिक प्रभाव असतो. [५७] ह्यांचे निकाल दर्शवतात की तरुण वापरकर्ते टंचाई (उदा. : `आयुष्यात येणारी एकमेव संधी' प्रकारचे संदेश) तर वयस्कर वापरकर्ते परस्परसंवादाला (उदा. : विनामूल्य भेटवस्तू चे आमिष दाखवून कुप्रणाली स्थापित करण्यास सांगणे) अधिक संवेदनशील असतात. [१४] ह्यांना आढळले की वापरकर्त्यांच्या कार्यभारामध्ये फरक आणि बिनमहत्त्वाच्या विपत्रांची संख्या, हे त्यांच्या सोंगजाळ्यांसंबंधित संवेदनशीलतेशी संबंधित आहेत. विश्वनाथ [७२] ह्यांनी वापरकर्त्यांचा फेसबुक वापराच्या सवयी आणि त्यांचा सोशल मीडिया वरील सोंगजाळ्यांसंबंधित संवेदनशीलतेचा अभ्यास केला. त्यांचे निकाल दाखवतात की नेहमीच्या फेसबुकच्या वापरामुळे होणारा प्रतिसाद स्वयंचलितपणा हा वापरकर्त्यांचा सोशल मिडिया वरील हल्ल्यांना बळी पडण्याचे एक प्रमुख कारक आहे.

सारांश असा, की विविध लोकसंख्येतील लोकांचे भिन्नविभिन्न मानसिक भेद्य असतात. वेगवेगळ्या वातावरणात लोकांना वेगवेगळ्या प्रकारच्या सवयी आणि धारणा असतात, आणि सोशल मीडियातील हल्ल्यांमध्ये नेहमीच्या वापरामुळे होणाऱ्या प्रतिसाद स्वयंचलितपणाची भूमिका महत्त्वाची आहे. वापरकर्त्यांचा आत्मविश्वास आणि परिणामाबद्दल त्यांचे मत देखील सोंगजाळ्यांसंबंधित संवेदनशीलतेशी संबंधित आहेत.

सोंगजाळ्यांविरोधी यंत्रणा

साहित्याबद्दलच्या आमच्या समजूतीवरून, सोंगजाळ्यांविरोधी यंत्रणांचे वृक्ष वर्गीकरण चित्र २.१ मध्ये दाखवल्याप्रमाणे दृश्यास्पद करता येऊ शकते. सोंगजाळ्यांना कमी करण्याच्या समाधानांचे थोडक्यात असे वर्गीकृत केले जाऊ शकते : अदृश्य करणे ; वापरकर्त्यांना शिकवणे ; उपयुक्त आंतरपृष्ठे विकसित करणे

प्रसंगणकांवर सोंगजाळी विपत्रांना ओळखण्याच्या नवगामी पद्धती ह्या मुख्यत्वे यंत्र स्वशिक्षणाच्या तंत्रांचा वापर करतात. संशोधकांनी मोठ्या प्रमाणात वैशिष्ट्यांची तपासणी केली आहे जी सोंगजाळी विपत्रांना ओळखण्यासाठी वापरली जाऊ शकतात [३, ३२]. ही वैशिष्ट्ये याप्रमाणे श्रेणीबद्ध करता येतात : संरचनात्मक, दुवे, घटक, अनपेक्षित विपत्रांसाठी चाळणी, शब्दार्थासंबंधी आणि डायनॅमिक मार्कोव्ह चेन. या प्रकारच्या वैशिष्ट्यांसह, संशोधकांनी विविध यंत्र स्वशिक्षणाच्या तंत्रांचे अन्वेषण केले आहे, जसे बॅग-ऑफ-वर्ड्स, बहु-वर्गीकरण, समूह, वर्गीकरण प्रतिकृती आधारित, बहु-थर, आणि उत्क्रांती संबंधक यंत्रणा [३, ३४, ३२]. नेटवर्क स्तरावर सोंगजाळ्यांना ओळखणे हे क्षेत्र आणि आयपी पत्ता काळ्यासुचींवर आधारित आहे, जसे डीएनएसबीएल आणि स्नॉर्ट. काही संशोधकांनी अशयाही यंत्रणा प्रस्थापीत केल्या ज्या प्रेषाकांच्या पार्श्वरेखा बनवून विपत्रात दर्शविलेल्या प्रेषकानेच विपत्र पाठवले आहे का, हे ओळखण्याचा प्रयत्न करतात [४१, ७०, २२]. विद्यमान साहित्यावरून हे लक्षात येते



आकृती २.१: सोंगजाळ्यांविरोधी यंत्रणांचे वर्गीकरण.

की सोंगजाळी संदेशांचा शोध घेण्यासाठी कुठली मानक वर्गीकरण पद्धत अस्तित्वात नाही आणि कुठलीही नवगामी पद्धत परिपूर्ण नाही. बहुसंख्य वर्गीकरण पद्धती पर्यवेक्षी शिक्षणावर आधारित असतात आणि जास्तं काम वास्तविक-वेळेमध्ये केले जात नाही. जरी नवगामी पद्धती काही हल्ल्यांना प्रत्यक्ष हल्ल्यावेळी शोधू शकत असले तरी त्यांचे चुकीचे-सकारात्मकचे अनिष्ट परिणाम सुद्धा असतात. संस्थात्मक वातावरणात आक्रमक तांत्रिक समाधानांचे नियोजन करताना चुकीचे-सकारात्मक यांचा मोठा बोजा असतो. उद्योगासंबंधित एका महत्वाच्या संदेशाला सोंगजाळी ठरवले तर व्यवसायावर गंभीर परिणाम होऊ शकतो.

विपत्र प्रमाणीकरण व पडताळणी तंत्रज्ञान (एसपीएफ, डीकेआयएम, डीमार्क) फसव्या विपत्रांशी लढा देण्यासाठी व्यवसायांसाठी आराखडा प्रदान करतात. ते अशा सोंगजाळी संदेशांना ओळखण्यासाठी वापरल्या जातात, जे बनावट प्रेषक पत्ते वापरून वैध संस्थांतून आल्याचे सोंग करतात. एसपीएफ हे धारकांना विपत्र पाठवण्यासाठी प्रेषाकच्या त्याच्या क्षेत्राचे कोणते प्रसंगणक वापरले जातात हे कळवते. डीकेआयएम हे प्रेषकाची संगणकीय स्वाक्षरी वापरून स्रोत आणि त्यातील मजकूराला प्रमाणित करते. डीमार्क हे अंतर्गत एसपीएफ आणि डीकेआयएम चा वापर करते, आणि विशालन क्षमता असलेली यंत्रणा निश्चित करते ज्याद्वारे प्रेषक त्याच्या क्षेत्रातून जाणारे विपत्र एसपीएफ आणि डीकेआयएम यांच्याशी पूर्णतः संरेखित न झाल्यास कसे हाताळावे याचा प्रस्ताव मांडते. परंतु, या तंत्रज्ञानाच्या अनेक त्रुटी आहेत आणि फॉर्च्यून ५०० मधल्या दोन-तृतीयांश संस्था ते वापरात नाहीत [१]. तरीही,

हे तंत्र बनावट विपत्र पत्त्यांसंबंधी हल्ले रोखू शकते, परंतु या व्यतिरिक्तच्या सोंगजाळ्यांना ते ओळखू शकत नाही.

डीएनएस-आधारित काळ्यासूची (डीएनएसबीएल) प्रसंगणकांद्वारे विपत्रांच्या उत्पत्तिस्थानाबद्दल जाणण्यासाठी वापरले जाऊ शकतात. काही डीएनएसबीएल, जसे स्पॅमहॉस डीबीएल, सोंगजाळी विपत्रांना पाठवणाऱ्या क्षेत्रांची नोंद ठेवतात आणि चुकीचे-सकारात्मकतेचा कमी दर ठेवण्याचा दावा करतात, जेणेकरून ते संस्थांच्या प्रसंगणकांवर वापरण्यासाठी कमी जोखमेचे असेल. डीएनएसबीएल यांच्यावर सामायिक प्रसंगणकांवरून आलेल्या वैध विपत्रांसमोर अडथला आणणे, आंतरजालीय सेवा प्रदातांच्या आयपी पत्त्याला बदलते ठरवून त्यांच्या कडून आलेले विपत्र योग्य नाहीत असे ठरवणे, इत्यादी अशा टीका झाल्या आहेत [१९].

एखादे नवीन संकेतस्थळ सोंगजाळी आहे की नाही हे दुव्यांचे आणि/किंवा एचटीएमएल चे विश्लेषण करून वर्गीकरण करता येते. दुव्यांचे वैशिष्टये शब्दरचने-आधारित आणि आयोजक-आधारित [७०]. शब्दरचनांची वैशिष्ट्ये दुव्यांचे शाब्दिक गुणधर्म आहेत. यजमान-आधारित वैशिष्ट्यांमध्ये संकेतस्थळाचे आयोजक कोण आहेत, संकेतस्थळाचे मालक कोण आहेत आणि तो कशा प्रकारे व्यवस्थापित केला जातो, या गोष्टी समाविष्ट असतात. ही वैशिष्ट्ये, एचटीएमएल-आधारित वैशिष्ट्यांसोबत नियम बनवण्यासाठी किंवा यंत्र स्वशिक्षण वर्गीकरण पद्धतींना प्रशिक्षण देण्यासाठी वापरले जातात. अनेक अभ्यासांत [६२, १३, ३३, ७६] सोंगजाळी संकेतस्थळांना ओळखण्यासाठी दुव्यांचे आणि एचटीएमएलचे विविध वैशिष्ट्ये वापरले गेले आहेत. [३९] ह्यांनी सोंगजाळी संकेतस्थळांना ओळखण्यासाठी दृश्यमान समानता आधारित पद्धतींचे विश्लेषण सादर केले आहे. [७५, ६३] हे सोंगजाळी संकेतस्थळ आणि वैध संकेतस्थळांतल्या दुव्यांतल्या संबंधांचा अभ्यास केला. २०१७ मध्ये, कुई इ. [१५] ह्यांनी दहा महिन्यांच्या कालावधीतल्या एकूण १९,०६६ सोंगजाळी हल्ल्यांचे निरीक्षण केले आणि असे आढळून आले की ९०% हल्ले इतर हल्ल्यांच्या प्रतिकृती आहेत. त्यांच्या समूहांचे निकाल असे दर्शवतात की हल्लेखोरांचा एक छोटा गट सध्याच्या बहुतांश हल्ल्यांच्या मागे असू शकतात. काही अभ्यासांनी वैध संकेतस्थळांची वैशिष्ट्ये श्वेतसुचींमध्ये साठवून त्यांची नवीन संकेतस्थळांशी तुलना केली आहे [१०, ५].

सोंगजाळी संकेतस्थळांची काळीसूची ही काळीसूची सेवा प्रदाताने सोंगजाळी ठरवलेल्या संकेतस्थळांची यादी असते. यापैकी सर्वात लोकप्रिय गुगल सेफ ब्राउजिंग, फिशटॅंक आणि एपीडब्ल्यूजी आहेत. गुगल ख्रोम, सफारी, फायरफॉक्स, ओपेरा आणि विवाल्डी सारखी आंतरजाल न्याहाळके गुगल सेफ ब्राउजिंग काळीसूची वापरतात [७७]. फिशटॅंक हा एक समुदाय आहे जेथे वापरकर्ते सोंगजाळी संकेतस्थळांची दुवे सादर करू शकतात, जे नंतर समुदाय मतदान वापरून सत्यापित केले जातात आणि त्यांच्या काळ्यासूचीत जोडले जातात. ही काळीसूची याहू मेल, मेकअफी, कासपर्स्की, एपीडब्ल्यूजी, ओपेरा आणि इत्यादी सारख्या संस्था आणि सेवा वापरतात [६१]. अँटी-फिशींग वर्किंग ग्रुप (एपीडब्ल्यूजी) एक आंतरराष्ट्रीय गट आहे जो सोंगजाळ्यांचा अहवालांना तयार करून त्याच्या देय

सदस्यांना वितरीत करतो[६०]. [६७] ह्यांना असे आढळून आले की वापरकर्त्यांना वास्तविक-वेळेमध्ये संरक्षण देण्यात काळ्यासूची निष्फळ ठरल्या, आणि त्या वेगवेगळ्या गती आणि व्याप्तीवर अद्यतनित केले गेले.

एकदा एखादे सोंगजाळी संकेतस्थळ सापडले, की त्याला बंद पाडण्यासाठी संबंधित सेवा प्रदाता अथवा आयोजकाकडे तक्रार नोंदवायची गरज असते. अनेक संस्था अश्या संकेतस्थळांची सेवा प्रदाताकडे तक्रार दकरण्याचा प्रयत्न करतात. संकेतस्थळ बंद पडण्याचा कालावधी सेवा प्रदाता वर अवलंबून असतो [६४]. फास्ट फ्लक्स नावाच्या एका हल्ल्याच्या पद्धतीत हल्लेखोर सोंगजाळी संकेतस्थळाला लपवण्यासाठी मोठ्या संख्येने तडजोड केलेले प्रॉक्सीच्या वापर करतात. [३६, १५] ह्यांच्या असे निदर्शनास आले की जरी सोंगजाळी संकेतस्थळ बंद पाडले तरीही हल्लेखोर वेगवेगळ्या क्षेत्रांतून, आयपी पत्ता आणि दुवे वापरून संकेतस्थळाला जास्तं सुधारित न करता हल्ला सुरु करतात. ते असे देखील दर्शवितात की काही हल्लेखोर गट मोठ्या संख्येने हल्ल्यांसाठी जबाबदार असतात, आणि वेगवेगळ्या हल्ल्यांसाठी समान संसाधने वापरतात. या गटांना ओळखल्याने मोठ्या संख्येने हल्ले रोखले जाऊ शकतात.

वापरकर्त्यांना शिक्षण आणि प्रशिक्षण ही आंतरजालीय सुरक्षिततेचा एक महत्त्वाचा भाग आहे, परंतु सोंगजाळ्यांविरोधी समुदायाकडून त्याला पुरेसे लक्ष मिळाले नाही. काही अभ्यासांनी दाखवले आहे की प्रशिक्षण कार्यक्रमे उपयुक्त ठरले आहेत [४५, ६६], तर काही याच्याशी असहमत आहेत किंवा असे म्हणतात की प्रशिक्षणाचे मिश्रित फायदे आहेत [११, ३०]. साहित्याच्या अभ्यासावरून असे कळते की सोंगजाळी हल्ल्यांच्या विरोधात प्रशिक्षण देण्याचा सर्वोत्तम मार्ग म्हणजे `प्रत्यक्ष वेळी - साहित्यापासून आमचे शिक्षण हे आहे की फिशिंग हल्ल्यांच्या विरोधात प्रशिक्षण देण्याचा सर्वोत्तम मार्ग म्हणजे ``प्रत्यक्ष क्षणी - नियतकालिक - विविध लोकसंख्येला अनुरूप" प्रशिक्षण [४६, ४५, ५७]. सोंगजाळ्यांविरोधात वापरकर्ता प्रशिक्षण संशोधनाचे छोटे खेळ किंवा अंतर्हित शिक्षण विकसित करण्यामध्ये श्रेणीबद्ध केले जाऊ शकते.

अँटी-फिशिंग फिल [६९] एक छोटा खेळ आहे जो वापरकर्त्यांना दुव्यांच्या विविध भाग आणि संकेतांबद्दल सांगून सोंगजाळी आणि वैध दुवे कसे ओळखायचे याचे शिक्षण देतो. ते हस्तक्षेप आधारित रचना तयार करण्यासाठी शिक्षणाच्या विज्ञानाचावापर करतात आणि त्यांना असे आढळून आले की त्यांची पद्धत ही उद्योगांद्वारे वापरल्या जाणाऱ्या सुरक्षितता सुचनांपेक्षा अधिक प्रभावी आहे. कंट्रोल-ऑल्ट-हॅक [१६] हे वापरकर्त्यांना एका तक्त्याच्या खेळत पत्त्यांसोबत खेळण्यास सांगतात, ज्याद्वारे ते वापरकर्त्यांना हल्लेखोरांकडून वापरल्या जाणाऱ्या वेगवेगळ्या सामाजिक अभियांत्रिकी पद्धतींबद्दल माहिती देतात. व्हॉट.हॅक [७४] हे वापरकर्त्यांना सामाजिक अभियांत्रिकी पद्धतींबद्दल माहिती देण्यासाठी कथा-आधारित खेळाच्या संदर्भातील कोडी सादर करते. काही व्यावसायिक उत्पादने उपलब्ध आहेत, जसे वुंबॅट सेक्यूरिटी द्वारे उपलब्ध ई-मेल सिक्युरिटी किंवा अँटी-फिशींग फिलीस [७८]. अंतर्हित

शिक्षणामध्ये वापरकर्त्यांच्या दैनंदिन प्राथमिक कामात शैक्षणिक साहित्य एकीकृत केले जाते. काही संस्थांनी, उदाहरणार्थ इंडियाना युनिव्हर्सिटी[३८] ह्यांनी वापरकर्त्यांना प्रशिक्षित करण्यासाठी नकली विपत्रे पाठवली आणि परिणामात वापरकर्त्यांच्या सोंगजाळ्यांना ओळखण्याच्या क्षमतेत सुधारणा दिसून आली. फिशगुरु [४४] मध्ये वापरकर्त्यांना सामान्य वापरामध्ये नकली विपत्रे पाठविल्या जातात आणि त्यांना प्रशिक्षित करण्यासाठी हस्तक्षेप आधारित शैक्षणिक संदेश वापरले जातात. जेव्हा वापरकर्ते हल्ल्याला बळी पडतात, जसे की सोंगजाळी विपत्रातल्या दुव्यावर टिचकी मारणे, तेव्हा प्रणाली वापरकर्त्यांना हल्ल्याबद्दल शिकवते.

योग्य संस्थात्मक धोरणे वापरकर्त्यांच्या तांत्रिक क्षमतांवर अवलंबून न राहता, संभाव्य हल्ले हाताळण्यास मदत करतात [३४]. संशोधकांनी अशा धोरणांसह सोंगजाळी-विरोधी आराखडे प्रस्तावित केले आहेत [२८]. तसेच काही आंतरराष्ट्रीय स्तरांवरील मानक आराखड्यांनी अशी धोरणे समाकलित केली आहेत [२] आणि काही राष्ट्रीय शासनांनी मार्गदर्शक तत्त्वेदेखील प्रस्तावित केली आहेत [५५].

संशोधनाची एक बाजू अधिक चांगले आंतरपृष्ठे विकसित करण्यावर भर देते जेणेकरून वापरकर्ते अशा प्रकारच्या हल्ल्यांविरूद्ध चांगले जाणीवपूर्वक निर्णय घेऊ शकतील. साहित्यातून आमचे शिकणे असे आहे की सावधानतेच्या संदेशांनी वापरकर्त्यांना अचूक संदेश दाखवून योग्य वेळी व्यत्यय आणावे आणि सवय लावू नये [३६, ७९, ६५, २४]. निष्क्रीय सूचक वापरकर्त्याला व्यत्यय आणत नाही. या सुचकांमध्ये काही विशिष्ट रंगाचे मजकूर आणि/किंवा चिन्ह असतात. उदाहरणार्थ, आंतरजाल न्याहाळकांतील सुरक्षा सूचके. संशोधनाने दर्शविले आहे की अनेक वापरकर्ते निष्क्रिय सुचकांकडे पाहत किंवा दुर्लक्ष करतात [७९]. [२५] ह्यांनी आकारमान, आकार, अर्थ लावणे यासारखे अभिकल्प निर्बंधांना लक्षात घेऊन तीन सुरक्षा निर्देशक प्रस्तावित केले. हे आता गुगल क्रोम ५३ पासून वापरले जातात. [८] ह्यांनी ``प्रतिबंधक आकर्षणे'' ह्यांची वस्तुरेखा मांडली, जे वापरकर्त्यांना सुरक्षा सूचनांमधील महत्वाच्या भागाकडे आकर्षित करतात जेणेकरून वापरकर्त्यांना अधिक माहितीपूर्ण निर्णय घेण्यास मदत होते. सक्रिय सूचक वापरकर्त्याच्या क्रियाकलापांना व्यत्यय आणतात. [५४] ह्यांनी विपत्रांमध्ये सामाजिक दक्षता टोकण्याच्या वापराचा प्रस्ताव मांडला. [२४, ७९] ह्यांनी दर्शविले की निष्क्रिय सुचकांपेक्षा सक्रिय सूचके अधिक प्रभावी असतात. वापरकर्ते सावधानतेच्या संदेशांकडे भाग पाडलेकी आणि समजण्याजोगे संदेश वापरले की लक्ष देतात. तसेच, सक्रिय सुचकांचे परिणाम त्यांच्या आखणी आणि अंमलबजावणीवर अवलंबून असतात. व्यत्यय हे सावधानतेच्या संदेशांची प्रभावीता वाढवत असल्याचे दाखविले आहे, परंतु हे व्यत्यय अगदीच वारंवार नसावे ज्याने वापरकर्त्यांना त्यांची सवय होऊन ते त्यांना दुर्लक्षियत करायला लागतील.

२.२ संबंधित कार्य

हो इ. [३५] ह्यांचे काम आमच्या कामाच्या सर्वात जवळचे आहे. त्यात लेखकांनी लाखातून एक आढळणाऱ्या ओळखमाहिती चोरणारे लक्ष्यित सोंगजाळे ओळखण्यासाठी एक प्रणाली विकसित केली. त्यांचे काम ३७ कोटी निनावी विपत्रांच्या एसएमटीपी, एनआयडीएस, एलडीएपी नोंदणीवर आधारित आहे. ते दर रात्री १० सर्वात संशयास्पद विपत्रांचे गुणानुक्रम करतात. १० हा आकडा त्यांच्या संस्थेतल्या विश्लेषकाने ठरवलेले बजेट आहे. ते सोंग करणाऱ्या तीन प्रकारच्या हल्ल्यांना तीन उप-प्रणालींद्वारे ओळखण्याचा प्रयत्न करतात. प्रत्येक उप-प्रणाली दोन टप्प्यांवर वर काम करते : आमिष आणि स्वार्थासाठी वापर. त्यांच्या दैनंदिन बजेटमध्ये त्यांनी ०.००५% इतका कमी चुकीचे-सकारात्मक दर प्राप्त केला. परंतु, ते सर्व हल्ल्यांच्या प्रसंगाचा शोध लावत नाहीत, म्हणून त्यांचा वास्तविक चुकीचे-सकारात्मक दर ज्ञात नाही. आम्ही प्रणाली त्यांच्या सारख्या प्रणालीच्या क्षमता वाढवेल, विशेषतः तिरकस लक्ष्यित सोंगजाळ्यांना शोधण्यासाठी.

आयडेनटीटी-मेलर [७०] हे प्रेषकांच्या विपत्र लिहिणे, रचना आणि प्राप्तकर्त्यांशी संवाद या सवयींवर आधारित त्यांच्या ऐतिहासिक पार्श्वरेखा तयार करते. प्रेषकाच्या बाजूला काम करताना ते येणाऱ्या विपतत्राची प्रेषकाच्या ऐतिहासिक पार्श्वरेखेशी तुलना करते. याच्या सारखेच, ईमेल-प्रोफाईलर [२२] हे प्राप्तकर्त्याच्या बाजूला काम करताना येणाऱ्या विपत्रांतून ऐतिहासिक पार्श्वरेखा तयार करते. ते विपत्राची अधिमाहिती व लिखाणाच्या शैलीचे वैशिष्ट्ये एसव्हीएम वर्गीकरण पद्धती सोबत वापरतात. संस्थेच्या गोपनीयतेबद्दलच्या शर्ती शिथिल असल्यास, विपत्रातील मजकुराचा वापर करून अश्या पद्धतींनी आमच्या प्रणालीला मदत मिळू शकते.

पेच्चीया इ. [७९] हे खात्यात प्रवेश करण्यानंतरच्या क्रियाकलापांचे विश्लेषण करून हल्ल्यांचा शोध लावण्याचा प्रयत्न करतात. ते एका बेझियान नेटवोर्कला प्रशिक्षण देण्यासाठी विविध सुरक्षा निर्देशक जसे की संशयास्पद कमांड-लाईन क्रियाकलाप, फाईल डाऊनलोड्स इत्यादी, यांचा वापर करतात. जरी त्यांनी त्यांच्या माहितीसंग्रहातील सर्व हल्ले ओळखले असतील, तरीही तसे करताना त्यांचे चुकीचे-सकारात्मक खूप जास्त प्रमाणात आले. लेखकांनी असे सुचवले आहे की त्यांची प्रणाली स्वतंत्ररीत्या चालण्यापेक्षा प्रशासकांना मार्गदर्शन करण्यासाठी अधिक योग्य आहे.

फ्रीमन इ. [२९] ह्यांनी खात्यात प्रवेश करण्याचे संशयास्पद प्रयत्न ओळखण्यासाठी एक सांख्यिकी बेझियन फ्रेमवर्क विकसित केले. ते प्रबलित प्रमाणीकरण याचा प्रस्ताव मांडतात, जे प्रमाणीकर्णासोबतच्या अतिरिक्त माहितीचा तपास करतात. ही अतिरिक्त माहिती ते एचटीटीपी सत्र नोंदणींतून मिळवतात. त्यांचा चुकीचे-सकारात्मक दर १०% इतका आहे, ज्याचे कारण जे व्यावसायिक निर्णय सांगतात. परंतु हा चुकीचे-सकारात्मक दर इतर संस्थांसाठी बराच मोठा आहे. प्रमाणीकर्णावरच काम करताना, झांग इ. [८०] ह्यांनी त्याच्या शैक्षणिक संस्थेतल्या प्रमाणीकरण नोंदणींतून वैशिष्ट्ये मि-

ळवत तर्कशास्त्र प्रतिगमन वर्गीकरण पद्धत वापरली.

लास्ज्का इ. [४९] ह्यांनी लक्ष्यित सोंगजाळ्यांना ओळखण्यासाठी खेळ सिद्धांताच्या संकल्पना वापरून योजनापूर्वक विपत्र अधःसीमेची निवड करण्याच्या समस्येवर काम केले. लेखक अशा प्रकरणाचा विचार करतात जिथे हल्लेखोर विविध घटकांकडे लक्ष देऊन निवडक लोकांना लक्ष्य बनवतात ज्याने त्यांन अधिकतम फायदा होईल. ते सैद्धांतिकदृष्ट्या सिद्ध करतात की की बचावफळी दीर्घकाळावर नॅश समतोल साधू शकतात. परंतु, ते कोणत्याही माहितीसंग्रहावर अशा प्रणालीचे कार्यप्रदर्शन सिद्ध करत नाहीत.

सोशल मिडियाच्या धर्तीवर, [२३, ७१] ह्यांनी मोठ्या प्रमाणावर प्रयोग केले ज्यामध्ये ते फेसबूक आणि ट्वीटर यांतल्या मजकूर आणि दुव्यांच्या सारखेपणावर आधारित समूह बनवतात. [२३] हे ऐतिहासिक पार्श्वरेखेचा विरूद्ध वापरकर्त्यांच्या वर्तनात विचलन पाहतात. तर [७१] हे वेगवेगळ्या प्रकारच्या खात्यांसाठी समूहांना श्रेणीबद्ध करण्यासाठी एक तर्कशास्त्र प्रतिगमन वर्गीकरण वापरतात. हे अभ्यास दर्शवितात की सोशल मेडिया वरील खाते हल्लेखोर प्रामुख्याने सोंगजाळ्यांद्वारे ताब्यात घेतात आणि अशी खाती मोठ्या प्रमाणावर सोंगजाळी मोहिमा आयोजित करण्यासाठी वापरले जातात. दीवान इ. [१७] लिंक्डइन या सोशल मिडिया वरच्या पार्श्वरेखांचे लिखाण शैली आणि सामाजिक वैशिष्ट्ये वापरून चार यंत्र स्वशिक्षण प्रणालींची तुलना करतात. परंतु, त्यांचे निकाल दाखवतात की लिंक्डइनमधील त्यांच्या निवडलेल्या वैशिष्ट्यांमुळे लक्ष्यित सोंगजाळ्यांना ओळखण्यात मदत झाली नाही.

प्रकरण ३

संकल्पना व आव्हाने

तिरकस लक्ष्यित सोंगजाळ्यांच्या हल्ल्यात प्रथम लक्ष्यित संस्थेतले एक खाते हल्लेखोर आपल्या ताब्यात घेतात. हे त्या हल्लेखोरांसाठी संस्थेत प्रवेश बिंदू आणि भक्कम पाया म्हणून कार्य करते. हल्लेखोर अनेक प्रकारे खात्याला ताब्यात घेऊ शकतात, जसे पासवर्ड चे brute force, चोरी, इत्यादी करून. संस्थेत हा पाया रचल्यानंतर हल्लेखोर त्या संस्थेत तिरकस प्रकारे हालचाल करत संवेदनशील माहितीच्या शोधात पुढे जाऊ शकतो. संवेदनशील माहिती मिळवण्यासाठी ताब्यात असलेल्या खात्याच्या संभाषणांची तपासणी करण्याच्या हेतूने हल्लेखोर निष्क्रिय देखील राहू शकतो. संशयास्पद क्रियाकलाप आढळून येईपर्यंत संस्थेत हल्लेखोराची उपस्थिती राहील. जरी दूरस्थ प्रवेश संस्थाच्या कार्यप्रवाहसाठी आवश्यक आहे, तरीही ते हल्लेखोराला संस्थेचा आवारात घुसण्याची संधी प्रदान करते. चोरी केलेली खात्यांची ओळखमाहिती काळ्या आंतरजालावर(डार्क वेब) प्रत्येकी सरासरीने $८ पासून जास्तीत जास्त $१९० पर्यंत विकली जाते [४३]. [८०] ह्यांना असे आढळून आले की विद्यापीठातली तडजोड केलेली खाती विद्वानिक लेख मिळवण्यासाठी आणि अभ्यवेक्षक टाळण्यासाठी वापरली जाऊ शकतात.

विपत्र खात्यांची तडजोड दोन टप्प्यांत शोधता येऊ शकते :

१. खात्यात प्रवेश करण्यावेळी ; प्रवेशाच्या क्रियाकलापांच्या गुणधर्मांचे विश्लेषण करून.
२. खात्यात प्रवेश केल्यानंतर ; विपत्र पाठवण्याचे क्रियाकलाप विश्लेषित करून.

दोन्ही टप्प्यांतील शोध प्रणालींचे फायदे आणि तोटे असतात, आणि त्या एकमेकांना पूरक असणे आवश्यक आहे. आमची प्रणाली दुसऱ्या टप्प्यावर काम करते. तडजोडीचा मार्ग विचारात न घेता आम्ही संशयास्पद विपत्र पाठवण्याच्या क्रियाकलापाचे विश्लेषण करतो. लक्ष्यात घ्या की आम्ही संस्थेच्या तडजोड केलेल्या खात्यातून केल्या जाणाऱ्या हल्ल्यांना तिरकस लक्ष्यित सोंगजाळे म्हणतो, वापर-

कर्त्याच्या वैयक्तिक विपत्र खात्यावरून केलेल्या हल्ल्याला नाही.

या हल्ल्यांना हाताळण्याचे एक आव्हान हे आहे की अशा घटना क्वचीत घडतात, ज्यामुळे ही समस्या गवतकाळात सुई शोधण्यासारखी असते. परंतु अशा हल्ल्यांमधील एक यशस्वी तडजोड संस्थांसाठी अत्यंत महागात पडू शकते. अशा क्वचोत घडणाऱ्या घटनांमुळे पायाभूत दराच्या समस्या येतात आणि माहितीसंच असंतुलित व लहान असतो. या समस्यांमुळे, मानक यंत्र स्वशिक्षण तंत्रज्ञानाचे यश असंभाव्य आहे. इतर समस्या अशा की वापरकर्त्यांचा मर्यादित इतिहास असणे आणि विपत्राच्या शीर्षभागाच्या मूल्यांमध्ये वैध घुसळण असणे, ज्यांनी मानक यंत्र स्वशिक्षण तंत्रज्ञानाचे निकाल आणखी खालावतात [३५]. आम्ही भाग ६.१ मध्ये आमच्या प्रणालीची तुलना यंत्र स्वशिक्षण तंत्रज्ञानाशी करून त्यांच्या परिणामांबद्दल अधिक चर्चा करतो.

आणखी एक आव्हान म्हणजे अंतर-क्षेत्रिय विपत्रांचे विश्वासाचे गुण अधिक असतात आणि त्यामुळे विसंगत असलेले विपत्रांना अडवले जात नाही [६८]. सोंगजाली विपत्रे जे सामान्यतः वैयक्तिक खात्यावरून पाठवले असता अडवले जातात, ते संस्थेतल्या खात्यावरून पाठवल्यास अडवले जात नाहीत, मुख्यतः अधिक विश्वासाच्या गुणांमुळे. आक्रमक नवगामींचा वापर मोठ्या प्रमाणात होत नाही कारण त्यांचे बऱ्याच वेळा चुकीचे-सकारात्मक आणि चुकीचे-नकारात्मक दर मोठे असतात जे संस्थेच्या उत्पादकतेला प्रभावित करतात. [५८]. वैध कर्मचारी-ते-कर्मचारी विपत्रे अनपेक्षित (स्पॅम) विपत्रांसारखे दिसू शकतात (उदा : मला ह्या गोष्टीवर सूट मिळाली, ह्या दुव्यावर टिचकी मारून तुला सुद्धा मिळवता येईल). हा वापरण्याच्या सहजतेचा मुद्दा आहे. अंतर-क्षेत्रिय विपत्रांच्या चाळणींची संवेदनशीलता संस्था प्रशासकाद्वारे सुधारित केली जाऊ शकते. परंतु त्यामध्ये चुकीचे-नकारात्मक चा धोका असतो आणि दैनंदिन प्रवाहात अडथळा न लावता चांगले परिणाम देण्यासाठी पुरेशा चाचणी ची गरज असते.

बहु-घटक प्रमाणीकरण हल्लेखोरांसाठी घुसखोरीसाठी लागणारी किंमत वाढवू शकते. परंतु, हे प्रमाणीकरण तंत्र उपयोजिततेच्या आणि उपयुक्ततेच्या समस्यांपासून ग्रस्त आहेत. या तंत्रज्ञानाची यश मुख्यत्वे त्याच्या अंमलबजावणीवर अवलंबून असते आणि हल्लेखोरांसाठी कमकुवत अंमलबजावणीवर मात करून पुढे जाण्यास जास्तं अडचण येत नाही [७]. विविध संस्थांना जसे विद्यापीठे आणि राष्ट्रीय प्रयोगशाळांना हे प्रमाणिकरण तंत्र पद्धतीचा अवलंब करणे कठीण वाटते [४०].

तिरकस लक्ष्यित सोंगजाळ्यांममुळे संस्थेत हिमावसणा सारखा प्रभाव पडू शकतो ज्याने हल्ल्याने होणारी हानी आणखी वाढते. आमच्या संस्थेत झालेल्या एका घटनेत, एक कर्मचाऱ्यांच्या खात्याची तडजोड झाल्यामुळे लाक्षियत सोंगजाळी विपत्रे वापरून विद्यार्थ्यांची खात्यांची तडजोड करण्यात आली. ही खाते पुढे आणखी हल्ले करण्यासाठी आणि खात्यांची तडजोड करण्यासाठी वापरली गेली. वर्तमान स्थितीत, संस्था मुख्यत्वे त्यांच्या वापरकर्त्यांच्या लक्ष्यित सोंगजाळ्यांच्या तक्रारींवर अवलंबून असतात. पुढील प्रकरणात आम्ही आमच्या माहितीसंग्रहाविषयी चर्चा करतो आणि त्याचे तपशील सादर करतो.

प्रकरण ४

माहितीसंग्रहाचे वर्गीकरण

कोष्टक ४.१: माहितीसंग्रहातील विपत्रांची संख्या

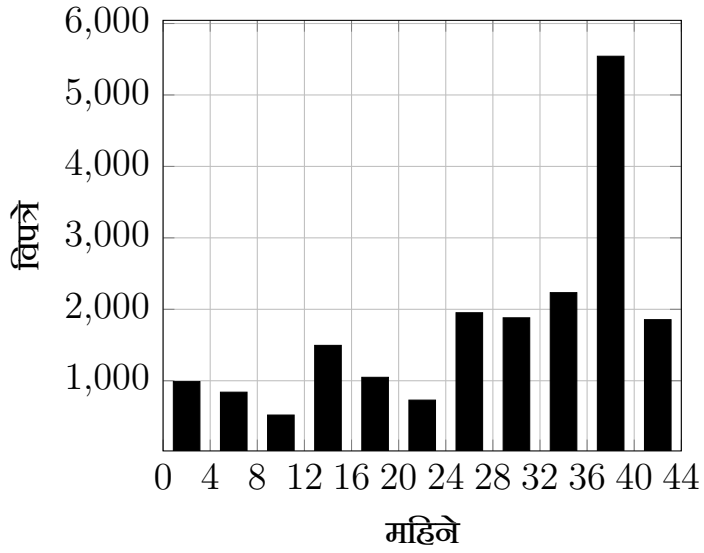
एकूण विपत्रे	११३,७२६
भिन्न विपत्रे	१९,०८७
भिन्न अंतर-क्षेत्रिय विपत्रे	१२,०६४

कोष्टक ४.२: सोंगजाळी दुवे आणि प्रदर्शित नाव फसवणूक संबंधित हल्ल्यांचे प्रसंग

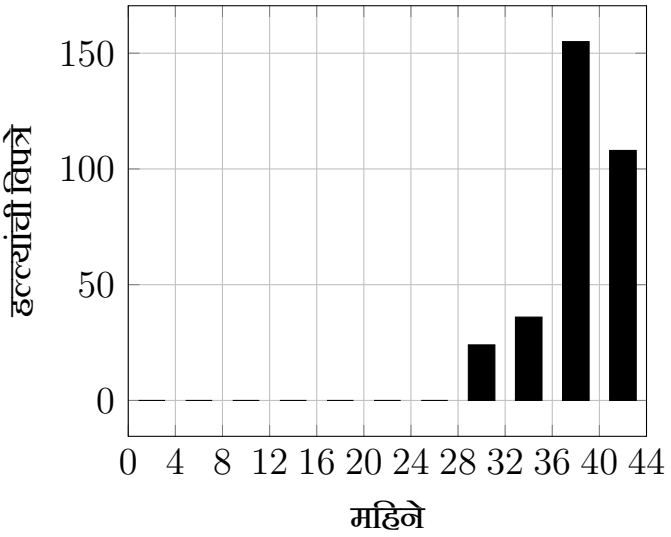
सोंगजाळी दुवे असलेले हल्ल्यांचे प्रसंग	२२/२७
प्रदर्शित नाव फसवणूक संबंधित हल्ल्यांचे प्रसंग	०४/२७

आमचे कार्य सीओईपी मधील स्वैच्छिकांकडून गोळा केलेल्या विपत्रांवर आधारित आहे. सीओईपी आपल्या विपत्रांच्या गरजेसाठी ऑफिस३६७ ओउटलूक वापरते. गोपनीयतेच्या कारणांमुळे आम्ही आमच्या संस्थेचा संपूर्ण विपत्रांचा इतिहास मिळवू शकलो नाही. त्यामुळे आम्ही संस्थेतल्या ४० स्वैच्छिकांकडून त्यांचे संस्थेतल्या खात्यांचे विपत्र गोळा केले. स्वैच्छिकांचे विपत्रे डाउनलोड करून त्यांना प्रक्रिया करण्यायोग्य स्वरूपनामध्ये रूपांतरित करण्यात आले. विपत्रांमध्ये त्यांच्या संबंधित शीर्षभाग (हेडर) आणि शरीर दोन्ही आहेत. माहितीसंग्रहात जुलै २०१४ ते जानेवारी २०१८ चे ३.५ वर्षांइतके विपत्रे आहेत. विपत्रांची एकूण संख्या आहे ११३,७२६ आहे. वैयक्तिक स्वैच्छिकांकडील विपत्रे एकत्रित केल्यावर आमच्या माहितीसंग्रहात १९,०८७ भिन्न विपत्रे आहेत. ह्यापैकी १२,०६४ हे अंतर-क्षेत्रिय विपत्रे आहेत. ह्याचे पुनरावलोकन कोष्टक ४.१ मध्ये केले आहे.

जरी आमच्याकडे संस्थेचे सर्व वैध विपत्रे नसले तरी आमच्या माहितीसंग्रहात सर्व ज्ञात हल्ल्यांचे प्रसंग असण्याचे आम्ही प्रयत्न केले. माहितीसंग्रहात विविध शैक्षणिक वर्षातल्या विद्यार्थ्यांच्या आणि काही



आकृती ४.१: माहितीसंग्रहातील ४ महिन्यांच्या मध्यांतरांनी भिन्न विपत्रे.



आकृती ४.२: माहितीसंग्रहातील ४ महिन्यांच्या मध्यांतरांनी भिन्न हल्ल्यांची विपत्रे.

शिक्षकांच्या विपत्रांचा इतिहास आहे. संस्थेतल्या एखाद्या खात्याची तडजोड केल्यानंतर हल्लेखोरांकडून लक्ष्यित सोंगजाळी हल्ल्यांचे प्रकार म्हणजे एकतर सीओईपी च्या संकेतस्थळासारखे सोंगजाळी संकेतस्थळ वापरून ओळखमाहिती चोरणे किंवा संस्थेतल्या इतर लक्ष्यितांची संवेदनशील माहिती मिळवण्यासाठी त्यांच्याशी संवाद साधणे.

आमच्या माहितीसंग्रहात हल्ल्यांच्या एकूण २७ घटना आहेत, ज्यापैकी २५ हे आम्हाला आधी ज्ञात होते आणि २ घटना हे आमच्या प्रणाली ने नंतर सापडवले. ह्या २७ घटना ३२३ विपत्रांशी निगडीत आहेत. एखाद्या खात्याची तडजोड झाली की त्याचा वापर संस्थेतल्या इतर लक्ष्यितांना लक्ष्यित सोंगजाळी

विपत्रे पाठवण्यासाठी केला गेला. वापरकर्त्यांनी प्रशासकीय गटाला हल्ल्याची तक्रार केल्यानंतर त्या खात्याचा प्रवेश रद्द केला जातो. ह्यातली काही लक्ष्यित सोंगजाळी विपत्रे इतरांना प्रशासकीय गटाचे सोंग करत मोठ्या प्रमाणात देखील पाठवले गेले. मोठ्या संख्येने पाठवले गेल्याने लक्ष्यित सोंगजाळी विपत्रांना किती वापरकर्त्यांनी प्रतिसाद दिला आहे हे माहित नाहीये.

कोष्टक ४.२ हे सोंगजाळी दुवे आणि प्रदर्शित नाव फसवणूक संबंधित हल्ल्यांचे प्रसंग दाखवते. सर्व सोंगजाळी संकेतस्थळे हे सीओईपीच्या संकेतस्थळाची नक्कल करणारे होते आणि सर्व प्रदर्शित नाव फसवणूक प्रसंगांमध्ये सीओईपीतल्या एखाद्या व्यक्तीची नक्कल केली गेली.

आमच्या माहितीसंग्रहात सर्व शैक्षणिक वर्षाच्या स्वैच्छिकांचे विपत्रे असल्यामुळे निरीक्षणाच्या कालावधीच्या शेवटी विपत्रांची संख्या अधिक आहे ; परंतु तेच सुरवातीच्या काळासाठी सत्य नाही. आकृती ४.१ ही ४ महिन्यांच्या मध्यांतरांनी आमच्या माहितीसंग्रहातील विपत्रांची संख्या दर्शविते. तसेच, आकृती ४.२ ही ४ महिन्यांच्या मध्यांतरांनी हल्ल्यांच्या विपत्रांची संख्या दर्शविते. २०१६ च्या उत्तरार्धापासून संस्थेत अशा हल्ल्यांची संख्या प्रचंड प्रमाणात वाढली आहे.

प्रकरण ५

मुल्यांकन प्रणालीची योजना

मुल्यांकन प्रणालीचा मुख्य उद्देश कमी चुकीचे-सकारात्मक दर आणि समाधानकारक खरे-सकारात्मक दर मिळवणे आहे. आणखी एक ध्येय असे की वास्तविक-वेळी असावे जेणेकरून विपत्रे येतील तसे त्यांच्यावर लगेच प्रक्रिया करता येईल. आम्ही विपत्राच्या शीर्षभागातील संरचित माहिती आणि विपत्राच्या शरीरातील एका घटकाचा वापर करतो. मुल्यांकन प्रणाली प्रत्येक प्राप्त विपत्रासाठी मूल्य निर्धारित करते आणि त्यानुसार घ्यावयाची कृती ठरवते. पुढील दोन विभाग आमच्या प्रणालीला देण्यात येणाऱ्या वैशिष्ट्यांचे आणि नंतर मुल्यांकन प्रणालीचे वर्णन करतात.

५.१ वैशिष्ट्यांचे वर्गीकरण

आम्ही आमच्या संस्थेतील तिरकस लक्ष्यित सोंगजाळी विपत्रांच्या निरीक्षणावरून ४ चार वैशिष्ट्य श्रेण्या साध्य करतो. प्रत्येक वैशिष्ट्याच्या श्रेणीमध्ये एक किंवा अधिक वैशिष्ट्ये आहेत. त्याच्या स्वभावावर आधारित, एखादे वैशिष्ट्य संदर्भ-आधारित किंवा इतिहास-आधारित असू शकते. संदर्भ-आधारित वैशिष्ट्य विपत्राच्या विशिष्ट गुणधर्म / संदर्भाचे विश्लेषण करते, तर इतिहास-आधारित वैशिष्ट्य ऐतिहासिकदृष्ट्या ज्ञात असलेल्या पार्श्वरेखेशी तुलना करतो.

५.१.१ वर्तन संदर्भांच्या वैशिष्ट्यांचा वर्ग

संस्थेतल्या एखाद्या खात्याची तडजोड झाली की हल्लेखोर संस्थेतील इतर अशा वापरकर्त्यांना लक्ष्यित सोंगजाळी विपत्रे पाठवू शकतात ज्यांचा खऱ्या वापरकर्त्याशी काही संबंध नाही. आम्ही हे वर्तन

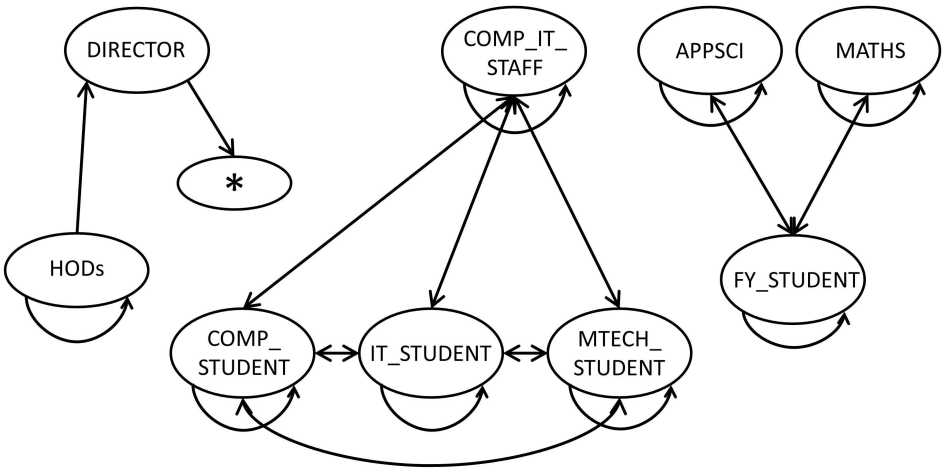
ओळखण्याचा प्रयत्न करतो. एक नैसर्गिक समाधान म्हणजे विपत्रांच्या इतिहासावरून वारंवार विपत्रे पाठवण्याचे प्ररूप (पॅटर्न) सापडवणे. परंतु, आम्ही या प्रकरणात नंतर स्पष्ट करतो की बाबतीत हे लागू होत नाही. आमची युक्ती आहे की प्रेषक आणि प्राप्तकर्त्यांदरम्यान `*अर्थपूर्ण*' संबंध आहे का हे तपासणे. फक्त संबंध नसून, 'अर्थपूर्ण' संबंध या संज्ञाची नोंद घ्यावी. अर्थपूर्ण संबंधाचे एक उदाहरण म्हणजे संगणक विभागाच्या शिक्षकांनी संगणक विभागातील विद्यार्थ्यांना विपत्र पाठविणे. तर संगणक विभागाच्या शिक्षकांनी धातुविज्ञान विभागातील विद्यार्थ्यांना विपत्र पाठवणे हे अर्थपूर्ण नाही. आधी आम्ही अर्थपूर्ण संबंध कसे स्थापित करतो ह्याचे वर्णन करतो.

आम्ही संस्थात्मक विपत्र पाठवण्याचा पदानुक्रम ही संकल्पना सादर करतो. हा पदानुक्रम बिंदू आणि जोडणींनी बनलेला आलेख आहे, जो संस्थेतील अर्थपूर्ण विपत्र पाठवण्याचे संबंध दाखवतो. बिंदू हे वैयक्तिक वापरकर्ते किंवा वापरकर्त्यांचे गट असू शकतात, आणि ते जोडण्या वापरून जोडले जातात. जोडण्या दिशात्मक आहेत. बिंदू अ कडून बिंदू ब कडे जाणारी जोडणी म्हणजे बिंदू अ चा बिंदू ब ला अर्थपूर्ण विपत्र पाठवण्याचा संबंध आहे. हेच उलटपक्षी लागू होत नाही जर बिंदू ब पासून बिंदू अ कडे जाणारी जोडणी नसेल.

जरी पदानुक्रमातील बिंदू वैयक्तिक वापरकर्ते असू शकतात, तरी पदानुक्रमाची गुंतागुंत कमी करण्यासाठी, बिंदू हे संस्थांमधील `समूह' असू शकतात (उदा. : संघ, वर्ग, विभाग इ.). स्थापित समूहापेक्षा जर त्यातील एखाद्या वापरकर्त्याला अधिक जबाबदारी / हक्क असतील (उदा. : संघ नेता, विभाग प्रमुख इ.), तर त्याला समूहासह स्वतंत्र बिंदू म्हणून मानले जाऊ शकते. अशा परिस्थितीत, एक वापरकर्ता एकाधिक बिंदूचा भाग असेल आणि अन्य त्यांचे इतर बिंदूंशी भिन्न जोडण्या असणार. पदानुक्रमात विविध पातळ्या / उपसंचांचा वापर केला जाऊ शकतो. एखाद्या संस्थेमधील एका विभागाशी संबंधित पदानुक्रम कसा असू शकतो याचे एक साधे उदाहरण आकृती ५.१ मध्ये दर्शविले आहे.

आम्ही याला विपत्र पाठवण्याचा पदानुक्रम असे म्हणतो आणि पाठवण्याचे प्ररूप नाही, कारण आम्ही फक्त वारंवार प्ररूप वापरत नाही. उदा. एखाद्या संस्थेचे संचालक संस्थातील विद्यार्थ्यांना वारंवार ईमेल पाठवत नसतील आणि पाठवण्याचा प्ररूप अनियंत्रित असू शकतो. परंतु हे एक अर्थपूर्ण संबंध आहे. यामुळे, प्रेषकाने प्राप्तकर्त्यास किती पूर्वीचे दिवस विपत्र पाठविले आहेत किंवा विपत्र पाठवण्याचे प्ररूप, फक्त यासारख्या घटकांकडे पाहून आम्ही विसंगती वर्तन ठरवू शकत नाही. म्हणूनच, आम्ही पदानुक्रमाची बांधणी करताना विपत्र पाठवण्याच्या अर्थपूर्ण संबंधांचा वापर करतो. प्रशासक अशा पदानुक्रमाची रचना करण्यासाठी त्यांचे क्षेत्रिय ज्ञान वापरू शकतात.

प्रशासक विपत्र पाठवण्याचे प्ररूप शोधण्यासाठी यंत्र स्वशिक्षण तंत्रांचा वापर करून संस्थेच्या विपत्रांच्या इतिहासाचा फायदा घेऊ शकतात. वर नमूद केल्याप्रमाणे, आम्ही `अर्थपूर्ण' प्ररूप शोधतो, फक्त वारंवार प्ररूप नाही. म्हणून, प्रशासक संस्थेच्या प्ररुपांची प्राथमिक दृश्य मिळवण्यासाठी स्वशिक्षण तंत्रांचा वापर करू शकतात आणि नंतर त्यांच्या गरजेनुसार बदलू शकतात. गोजेएस (GoJS), सिग्मा-



आकृती ५.१: एका संस्थेतील संगणक विभागासंबंधित पदानुक्रमाचे उदाहरण. नोंद : ही आकृती कोणत्याही पदानुक्रमाची प्रतिनिधी नाही आणि केवळ पदानुक्रमाची संकल्पना स्पष्ट करण्यासाठी वापरली आहे. संस्था त्यांच्या मर्जीनुसार पदानुक्रमाचे स्वरूप ठरवू शकतात.

जेएस (SigmaJS), विजजेएस (VisJS) सारखे जावास्क्रिप्ट कार्यसंचांच्या सहाय्याने (किंवा पसंतीच्या कोणत्याही संगणकीय भाषेत उपलब्ध असलेले कार्यसंच) पदानुक्रम माहितीसाच्यात (डेटाबेस मध्ये) सहजपणे जतन केले जाऊ शकतात. हे एक संदर्भ-आधारित वैशिष्ट्य आहे जे प्रेषकाने त्याच्या प्राप्तकर्त्यांना विपत्र पाठविणे `अर्थपूर्ण 'आहे किंवा नाही हे तपासते. येथे वैध अपवाद असू शकतात जेथे विपत्र पाठविण्यात अर्थपूर्ण संबंध नसतील, परंतु असे संभवतः दुर्मिळ आहेत.

संस्थेच्या आधारावर या श्रेणीमध्ये अधिक वैशिष्ट्ये जोडले जाऊ शकतात. उदाहरणार्थ, आमच्या बाबतीत, जर विपत्रासाठी पदानुक्रमात जोडणी नसेल आणि प्राप्तकर्ते विपत्राच्या बीसीसी (Bcc) मध्ये असतील, तर आम्ही त्याला अधिक संशयास्पद समजतो.

५.१.२ आय.पी. वैशिष्ट्यांचा वर्ग

एखाद्या खात्याची तडजोड जगातील कुठूनही होऊ शकतो. कार्यक्षमते आणि सहजपणे वापरण्यासाठी, संस्थात्मक वापरकर्त्यांना दूरस्थपणे त्यांच्या खात्यांमध्ये प्रवेश करण्याची परवानगी दिली जाते. परंतु, हे हल्लेखोरांसाठी देखील घुसखोरी करण्याची संधी प्रदान करते. हा वैशिष्ट्य वर्ग एक ज्ञात भौगोलिक स्थानावरून विपत्र पाठविले आहे किंवा नाही हे तपासतो. ही तपासणी संथात्मक-व्यापी तसेच प्रति-वापरकर्ता असे दोन्ही आहे. या वर्गातील पहिले वैशिष्ट्य हे भौगोलिक-आयपी माहितीसाच्याकडून प्राप्त प्रेषकच्या शहरावर आधारित आहे. या वैशिष्ट्याचे पुढे दोन उप-वैशिष्ट्ये आहेत.

१. प्रेषकाने त्या शहरातून विपत्र पाठविण्याची संख्या, आणि
२. त्या शहरातून विपत्र पाठवलेल्या इतर वापरकर्त्यांची संख्या.

दोन्हींमध्ये, छोटा आकडा म्हणजे अधिक संशयास्पद असणे. एक अशी परिस्थिती उद्भवू शकते जिथे त्या शहरातून प्रेषकाने पुरेसे विपत्र पाठवले आहेत, परंतु तेथे पुरेसे वापरकर्ते नाहीत ज्यांनी त्या शहरातून विपत्र पाठविले आहेत. हे त्यावेळी होऊ शकतं जेव्हा तो वापरकर्ता त्या शहराला अनेक वेळा भेट देत असेल. त्यामुळे, जर पहिल्या उप-वैशिष्ट्याने पुरेसा मोठा आकडा दिला, तर प्रणाली दुसऱ्या उप-वैशिष्ट्याच्या आकड्याकडे दुर्लक्ष करते. तरीही, दुसरे उप-वैशिष्ट्याचे मुख्य उद्देश आहे, कारण आमच्या संस्थेतील अनेक विद्यार्थी क्वचितच विपत्र पाठवतात. त्यामुळे प्रति-वापरकर्ता ऐतिहासिक त्यामुळे प्रति-वापरकर्ता ऐतिहासिक पार्श्वरेखा पुरेशी तयार होत नाही. अशा परिस्थितीत, हे संथात्मक-व्यापी उप-वैशिष्ट्य त्या शहरातून विपत्र पाठविणाऱ्या वापरकर्त्यांची संख्या सांगत प्रमुख भूमिका निभावते. आम्ही विविध भौगोलिक-आयपी माहितीसाच्यांची चाचणी केली आणि आम्हाला आढळले की IP२Location आमच्या बाबतीत इतर सेवांच्या तुलनेत अधिक अचूक अनुबंध देते, व त्यानंतर MaxMind.

शहर-आयपी अनुबंध पूर्णपणे विश्वासार्ह नसते आणि काही परिस्थितींमध्ये चुकीचे अनुबंध देते. म्हणून आम्ही या वर्गामध्ये दुसरे वैशिष्ट्य वापरतो, जे आयपी-एएसएन अनुबंधापासून प्राप्त एएसएन वर आधारित आहे (ऑटोनोमस सिस्टम नंबर - एका आंतरजालीय सेवा प्रदाता च्या अंतर्गत आयपी पत्त्यांच्या संचासाठी अभिज्ञापक/क्रमांक). एएसएन चे व्याप हे बहुतांश वेळा शहरापेक्षा छोटे असते आणि कधीकधी उलटपक्षी. तरी तो वास्तविक वापरासाठी चांगला पर्याय आहे. शहर आधारित उप-वैशिष्ट्यांसारखेच, या वैशिष्ट्यामध्ये दोन उप-वैशिष्ट्ये आहेत.

१. प्रेषकाने त्या एएसएन मधून विपत्र पाठविण्याची संख्या, आणि
२. त्या एएसएन मधून विपत्र पाठवलेल्या इतर वापरकर्त्यांची संख्या.

वर्णित शहर आधारित उप-वैशिष्ट्यांप्रमाणे, इथे देखील जर पहिल्या उप-वैशिष्ट्याने पुरेसा मोठा आकडा दिला, तर प्रणाली दुसऱ्या उप-वैशिष्ट्याच्या आकड्याकडे दुर्लक्ष करते. आयपी-एएसएन अनुबंधासाठी आम्ही MaxMind चा एएसएन माहितीसाचा वापरतो.

या वर्गामधील दोन्ही वैशिष्ट्ये इतिहास-आधारित आहेत.

जेव्हा एखादा वैध वापरकर्ता प्रवास दरम्यान विपत्र पाठवितो तेव्हा समस्या निर्माण होते. वापरकर्ता प्रवास करत आहे किंवा नाही हे निर्धारित करण्यासाठी, जावेद [४०] ने वापरकर्ता खात्यात प्रेअवेश मिळवण्यासाठी विमानतळाच्या वायफाय वापर करतोय का हे जाणण्यासाठी विमानतळांच्या एएसएन चा वापर केला आहे. परंतु सार्वजनिक ठिकाणी असलेल्या अशा असंख्य एएसएन श्वेतसूचीमध्ये असतील तर हल्लेखोरांद्वारे याचा गैरफायदा घेतला जाऊ शकतो. आणि आमच्या बाबतीत अशा अनेक शक्यता

आहेत जसे की ट्रेन, बस इ. मधील सार्वजनिक वायफाय. त्यामुळे आम्ही वापरकर्त्याच्या प्रवासाच्या प्रसंगाला समाविष्ट न करण्याचा निर्णय घेतला.

आमच्या संस्थेतील बदलत्या आयपी पत्त्यांमुळे आणि खात्यात दूरस्थपणे प्रवेश करणाऱ्या वापरकर्त्यांमुळे, आम्ही वापरकर्त्याने आधी त्या आयपी पत्त्याचा वापर केला आहे किंवा नाही हे तपासू शकत नाही. संस्थेमधील विविध प्रसंगी वापरकर्त्याच्या संगणकाला वेगवेगळे आयपी देण्यात येऊ शकते.

५.१.३ प्रदर्शित नाव वैशिष्ट्यांचा वर्ग

तिरकस लक्ष्यित सोंगजाळी हल्ल्यांमध्ये प्रदर्शित नाव फसवणुकीच्या पद्धती देखील वापरले जाऊ शकतात. पूर्वीच्या विविध अभ्यासांमध्ये दाखवल्याप्रमाणे [४, ६], तांत्रिकदृष्ट्या ज्ञात लोकं देखील प्रदर्शित नाव फसवणुकीला बळी पडू शकतात. उदाहरणार्थ, एका विद्यार्थ्याचे तडजोड झालेल्या खात्याला प्रयोगशाळा सहाय्यक चे नाव देण्यात येनु शकते (संगणक प्रयोगशाळा सहाय्यक <studentemailid@coep.ac.in>). प्रेषक हा खरंच प्रयोगशाळा सहाय्यक असल्याचे समजून प्राप्तकर्ते त्या विपत्राला प्रतिसाद देतील.

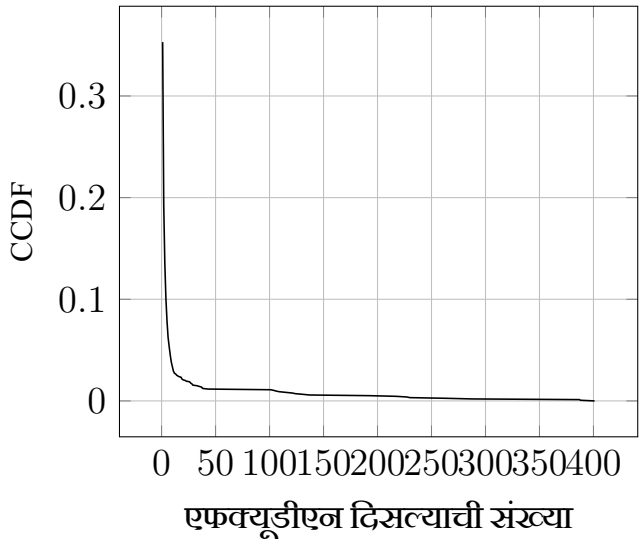
एसपीएफ / डीकेआयएम / डीमार्क [५३] सारखे प्रमाणीकरण तंत्र या बाबतीत कमी येत नाहीत कारण विपत्र हे अंतर-क्षेत्रिय असते आणि वैध खात्यातून पाठवले जाते.

या श्रेणीतील पहिले वैशिष्ट्य प्रेषकाने वर्तमान प्रदर्शित नावासह विपतत्रे पाठवलेल्या प्रसंगांची संख्या देते. हे इतिहास-आधारित वैशिष्ट्य आहे.

संस्थेतील अनेक विद्यार्थी क्वचितच विपत्र पाठवतात. म्हणून, अशा विद्यार्थ्यांसाठी प्रदर्शन नावाची पुरेशी नोंद नसते. या वर्गामधील दुसरे वैशिष्ट्य प्रेषकसाठी वर्तमान प्रदर्शन नावांची अपुरी नोंद असल्यास प्रदर्शित नावाची शब्दरचना विपत्र पत्त्याप्रमाणे आहे किंवा नाही हे तपासते. बहुतांश वेळी, संस्था त्यांच्या वापरकर्त्यांचे विपत्र पत्ते हे त्यांच्या वास्तविक नावावर आधारित असते. त्यामुळे जरी विपत्र पत्त्यात अचूक नाव नसले तरी शब्दरचने आधारित तुलना यशस्वीरीत्या कार्य करू शकते. उदा. : आमच्या संस्थेत विपत्र पत्त्यात वापरकर्त्याच्या नावाचा एखादा भाग असतो (नाव आणि / किंवा आडनाव). आम्ही या संरचनेचा वापर प्रेषकाच्या विपत्र पत्त्या आणि प्रदर्शन नावाशी तुलना करण्याच्या दृष्टीने करतो. हे संदर्भ-आधारित वैशिष्ट्य आहे.

आम्ही फसवणूक केलेल्या प्रदर्शन नावाची विश्वासार्हता / प्रतिष्ठा लक्षात घेत नाही कारण आम्हाला अशी उदाहरणे आढळली जिथे लोक

आम्ही स्पूफ्ड डिस्प्ले नावाची विश्वासार्हता / प्रतिष्ठा लक्षात घेत नाही कारण आमच्याकडे अशी उदा-



आकृती ५.२: आमच्या माहितीसंग्रहात एखादे एफक्यूडीएन दिसल्याच्या संख्येचे पूरक संचयी वितरण फल. *पूरक संचयी वितरण फल (Complementary cumulative distribution function - CCDF)

हरणे आहेत जिथे वापरकर्ते अधिकारी / ज्ञात प्रदर्शन नावांचा वापर न होता या हल्ल्यांना बळी पडले आहेत.

५.१.४ एफ.क्यू.डी.एन. वैशिष्ट्यांचा वर्ग

कोष्टक ४.२ मध्ये दाखवल्याप्रमाणे, आमच्या माहितीसंग्रहातील २२ हल्ल्यांत विपत्रामध्ये सोंगजाळी दुवा आढळल्या. दुव्यांमध्ये मध्ये बरेच फरक असू शकतात, जसे की दुव्यामधील विविध मापदंड. संपूर्ण दुवा वापरण्याऐवजी, आम्ही एफक्यूडीएन (Fully Qualified Domain Name - FQDN), जो दुव्याचा शीर्ष-भाग असून, त्याचा वापर करतो. एफक्यूडीएन वापरल्याने सूक्ष्मतेला हाताळता येते आणि ते खूप भरड ही नसते. उदा. : http ://wwww.en.coep.org.in/departments/computerit ?q=aniket&type=search या दुव्यात wwww.en.coep.org.in हे एफक्यूडीएन आहे. आम्ही असे मानतो की संस्थेसाठी नवीन एफ-क्यूडीएन हे अधिक धोकादायक असू शकते. पहिले वैशिष्ट्य हे तपासते की एफक्यूडीएन संस्थेत प्रथमच पाहिले जात आहे किंवा नाही. आम्हाला असे निदर्शनास आले की, आमच्या माहितीसंग्रहातले बहुतांश एफक्यूडीएन हे संपूर्ण निरीक्षण कालावधीमध्ये केवळ एकदाच दिसतात. कोष्टक ५.२ मध्ये दाखवल्याप्रमाणे, केवळ ३५% एफक्यूडीएन एकापेक्षा अधिक वेळा आढळल्या. दुसऱ्या शब्दात, ६५% एफक्यूडीएन फक्त एकदाच पाहिले गेले.

या वस्तुस्थितीमुळे, आम्ही फक्त एफक्यूडीएन चा संस्थेशी परिचय हे वैशिष्ट्य म्हणून वापरू शकत नाही. आणि याचा हल्लेखोरांद्वारे सोंगजाळी एफक्यूडीएन समाविष्ट असलेले विपत्र मोठ्या संख्येने

कोष्टक ५.१: मुल्यांकन प्रणालीला देण्याजाणाऱ्या वैशिष्ट्यांचा सारांश

वैशिष्ट्य	**स्वभाव**
वर्तन संदर्भांच्या वैशिष्ट्यांचा वर्ग	
पदानुक्रमात बिंदुंमध्ये जोडणी	संदर्भ-आधारित
प्राप्तकर्ते बीसीसी मध्ये	संदर्भ-आधारित
आय.पी. वैशिष्ट्यांचा वर्ग	
शहर वैशिष्ट्ये	इतिहास-आधारित
एएसएन वैशिष्ट्ये	इतिहास-आधारित
प्रदर्शित नाव वैशिष्ट्यांचा वर्ग	
प्रदर्शित नावाचा इतिहास	इतिहास-आधारित
शब्दरचनेशी तुलना	संदर्भ-आधारित
एफ.क्यू.डी.एन. वैशिष्ट्यांचा वर्ग	
संस्थेशी परिचय	इतिहास-आधारित
संस्थेतील प्रतिष्ठा	इतिहास-आधारित

पाठवून ते एफक्यूडीएन संस्थेसाठी परिचयाचे करून गैरफायदा घेता येऊ शकतो. आम्ही एफक्यूडीएन यांचा *संस्थेतील प्रतिष्ठेचा* मागोवा ठेवतो. जर वर्तमान विपत्रातील एफक्यूडीएन संस्थेत आधी दिसले असेल, तर आम्ही आमच्या दुसऱ्या वैशिष्ट्याचा वापर करतो, हे त्या एफक्यूडीएन ची संस्थेतील प्रतिष्ठा तपासतो. एफएक्यूडीएन च्या प्रतिष्ठेला आम्ही त्या विपत्राच्या संशयिते वरून परिभाषित करतो.

आम्ही पेजरॅंक (PageRank) इत्यादीसारख्या क्षेत्रिय प्रतिष्ठा वापरत नाही, कारण हल्लेखोर प्रतिष्ठित क्षेत्रावर त्यांचे पृष्ठ यजमानीत करू शकतात (उदा : Weebly, wordpress, इत्यादी). आमचे हे दुसरे वैशिष्ट्य एफक्यूडीएन चे संस्थेतील आत्तापर्यंतची प्रतिष्ठा देते. एफक्यूडीएनची प्रतिष्ठा ते आढळलेल्या विपत्रांच्या मुल्यांवर अवलंबून असते. एफक्यूडीएनच्या प्रतिष्ठेची गणना ही पुढच्या भागात वर्णीत केली आहे जिथे आम्ही मुल्यांकन प्रणालीचे वर्णन करतो. जर एखादे सोंगजाळी एफक्यूडीएन अधिक वेळा आढळले जात असेल तर पहिले वैशिष्ट्य अपयशी ठरेल, परंतु आम्ही एफक्यूडीएन च्या प्रतिष्ठेचा मागोवा ठेवल्याचा फायदा होईल.

या वर्गातील दोन्ही वैशिष्ट्ये इतिहास-आधारित आहेत. आम्ही विपत्राच्या शरीरातील इतर मजकूर वापरत नाही. आम्ही फक्त विपत्राच्या शरीरात असलेल्या कोणत्याही दुव्याचे एफक्यूडीएन वापरतो.

आम्ही कोष्टक ५.१ मध्ये सगळे वैशिष्ट्ये सारांशित केले आहेत.

५.२ ति.ल.सो. मुल्यांकन

मागील विभागात, आम्ही वैयक्तिक विपत्राला वैशिष्ट्यीकृत करण्यासाठी वापरतो त्या वैशिष्ट्यांचे वर्णन केले आहे. आता आम्ही एका विपत्राला मूल्य देण्यासाठी आणि त्याच्या अनुरूप कारवाई करण्यासाठी वैशिष्ट्य वर्गांना एकत्रित कसे करतो, याचे वर्णन करतो. साधेपणासाठी, आम्ही तिरकस लक्ष्यित सोंगजाळे याला ति.ल.सो. म्हणून संक्षिप्त करतो, म्हणून मुल्यांकन प्रणालीला ति.ल.सो. मुल्यांकन असे म्हटले जाते.

मुल्यांकन प्रणाली ०.० ते १.० च्या श्रेणीमध्ये अंतिम मूल्य देते. उच्च मूल्य म्हणजे विपत्राचे अधिक संशयास्पद असणे. आम्ही ०.५ पेक्षा अधिक मूल्याला तिरकस लक्ष्यित सोंगजाळी निर्धारित करतो. सर्व वैशिष्ट्य वर्गांच्या मूल्यांची साधी बेरीज करून एक अंतिम मूल्य मिळते. प्रत्येक वैशिष्ट्य वर्गाला त्याचे मूल्य त्याच्या वैयक्तिक वैशिष्ट्याच्या मूल्यांपासून मिळते. प्रत्येक वैशिष्ट्य वर्गाचे जास्तीत जास्त स्वीकार्य मूल्य असे असते की जेणेकरून ते ०.५ ओलांडत नाही. फक्त एक वैशिष्ट्य वर्ग विपत्राला तिरकस लक्ष्यित सोंगजाळी वर्गीकृत नाही यासाठी असे सुनिश्चित केले आहे. त्यामुळे, एखाद्या विपत्राला तिरकस लक्ष्यित सोंगजाळी वर्गीकृत करण्यासाठी, किमान दोन वैशिष्ट्य वर्गांकडून अशुन्य मूल्य मिळणे आवश्यक आहे. वैयक्तिक वैशिष्ट्य वर्गांची मुल्ये त्यानुसार सामान्यीकृत केले जातात.

संस्थेतील प्रशासकांनी ठरवलेल्या प्रत्येक इतिहास-आधारित वैशिष्ट्याच्या स्वतःच्या अधःसीमा आहेत. जर एखाद्या इतिहास-आधारित वैशिष्ट्याद्वारे दिलेले मूल्य त्याच्या अधःसीमे पेक्षा अधिक असेल, तर त्याला कोणतेही मूल्य मिळत नाही. मूल्य हे कमी होणाऱ्या ऐतिहासिक आकड्यांसोबत सोबत एकमिती ने वाढत जातात.

विपत्रासाठी तिलसो मूल्याची गणना झाल्यानंतर, विपत्राच्या शरीरातील एफक्यूडीएन यांची प्रतिष्ठा पुनःगणना होते. ही प्रतिष्ठा वर्तमान विपत्राचे मूल्य आणि एफक्यूडीएनची आत्तापर्यंतची प्रतिष्ठा, यापूर्वीच्या एफक्यूडीएन प्राप्त झालेल्या दिवसांची संख्येसोबत भारीत सरासरी करून मिळवली जाते. पुढच्या वेळी हे एफक्यूडीएन दिसल्यावर ही नवीन प्रतिष्ठा वापरली जाते.

आयपी, प्रदर्शित नाव सारख्या वैशिष्ट्यांना ऐतिहासिक पार्श्वरेखा तयार करून अचूक निर्णय देण्यासाठी पूर्व इतिहासाची आवश्यकता असते. या इतिहासावर आधारित वैशिष्ट्यांसाठी प्रारंभाची प्रक्रिया (bootstrapping) कालावधीची गरज असते. अधिक इतिहासामुळे प्रणालीच्या अधिक अचूक निर्णय देण्याच्या शक्यता वाढतात, तरीही त्याचा अर्थ असाही होईल की चांगल्या निर्णयांसाठी प्रणालीला बऱ्याच इतिहासाची गरज आहे. या प्रकरणात समतोल साधने आवश्यक आहे जेणेकरून पर्याप्त प्रमाणात इतिहासाचा वापर होईल, जे अतिरिक्त नसेल. याला अनुसरून, आमच्या प्रशिक्षण माहितीसंग्रहात सुरुवातीच्या ४ महिन्यांचे विपत्रे आहेत.

Algorithm 1: LSP Scoring

```
process_email(email E):
    F ← parse_fields(E)
    s1 ← get_behav_score(F[sender emailid, receivers])
    s2 ← get_ip_score(F[sender ip])
    s3 ← get_dn_score(F[sender emailid, sender displayname])
    s4 ← get_fqdn_score(F[fqdns])
    lsp_score ← s1 + s2 + s3 + s4
    if lsp_score > 0.5 then
        flag email
        update tables except history-based tables
    else
        update all tables
    return lsp_score
```

या प्रारंभ प्रक्रियेच्या काळात, जरी आयपी आणि प्रदर्शित नावांचा इतिहास बांधला जाईल, तरी विपत्रातील दुव्याची एफएक्यूडीएन प्रतिष्ठा निश्चित करणे देखील आवश्यक आहे. एफक्यूडीएन प्रतिष्ठा विपत्रांच्या तिलसो मुल्यांवरून मिळवली जातात. प्रारंभ प्रक्रियेच्या काळात, जर आम्ही ऐतिहासिक पार्श्वरेखांच्या पूर्व-अस्तित्वविनाच तिलसो मूल्याची गणना केली तर आम्हाला मोठ्या प्रमाणात चुकीचे-सकारात्मक मिळतात. हे प्रामुख्याने कारण आयपी आणि प्रदर्शित नावाच्या इतिहासाच्या कमतरतेमुळे होते. तसेच, या सुरवातीच्या विपत्रांमधील निर्दोष एफएक्यूडीएन यांना खराब प्रतिष्ठा प्राप्त होते आणि चुकीचे-सकारात्मक दराला आणखी वाढवतात. ही इतिहास बांधण्याची समस्या सोडवण्यासाठी आम्ही आम्ही प्रशिक्षण टप्प्यात दोन चरण वापरतो. पहिल्या चरणात, आम्ही सुरुवातीच्या चार महिन्यांच्या विपत्रांचा वापर आयपी आणि प्रदर्शित नावांचा इतिहास बांधण्यासाठी वापरतो. नंतर दुसऱ्या चरणात, आम्ही त्याच चार महिन्यांच्या विपत्रांचे तिलसो मुल्यांची गणना करतो (माहितीसाच्यातल्या आयपी आणि प्रदर्शित नावांच्या कोष्टकांचा फक्त संदर्भ घेतला जातो आणि ते अद्ययावत केले जात नाहीत, कारण ते पहिल्या चरणात माहितीसाच्यात भरले गेले असतात). जसे तिलसो मुल्यांची गणना होत जाते, विपत्राच्या शरीरातील एफएक्यूडीएन प्रतिष्ठा यांना माहितीसाच्यात अद्ययावत केले जाते. एकदा माहितीसाचा प्रशिक्षण विपत्रांच्या आयपी, प्रदर्शित नाव आणि एफएक्यूडीएन प्रतिष्ठांनी भरला

गेला, की आम्ही प्रणालीला प्रारंभ प्रक्रियेच्या कालावधीनंतरच्या विपत्रांवर चालवतो.

आमच्या स्थितीत, सर्वोत्तम प्रदार्षण देणाऱ्या भौगोलिक-आयपी माहितीसाच्यात देखील त्रुटी होत्या. यामुळे, चुकीच्या शहराच्या पुरेशा इतिहासाच्या अनुपस्थितीमुळे आयपी वैशिष्ट्य वर्गातील शहर वैशिष्ट्य अधिक मूल्य देते. आयपी-एएसएन माहितीच्यात खूप कमी चुकीची त्रुटी होत्या. म्हणूनच, जर शहर वैशिष्ट्य अशून्य मूल्य डेट असेल, परंतु एएसएन वैशिष्ट्य शून्य देत असेल, तर आम्ही आयपी वैशिष्ट्य वर्गाचे संपूर्णपणे शून्य मूल्य असल्याचे मानतो. आम्ही असे गृहीत धरतो की जर एएसएन-साठी पुरेशी ऐतिहासिक पार्श्वरेखा असेल, तर संबंधित शहरासाठी सुद्धा पुरेशी ऐतिहासिक पार्श्वरेखा असणे आवश्यक आहे.

एखादा हल्लेखोर विसंगती आयपी वरून आणि/किंवा प्रदर्शित नाव फसवणूक वापरत मोठ्या संख्येने विपत्रे पाठवून आमच्या ऐतिहासिक पार्श्वरेखांना दुषित करण्याचा प्रयत्न करू शकतो. म्हणून, जर एका विपत्राचे मूल्य ०.५ पेक्षा जास्त असेल तर आम्ही त्याच्या इतिहास आधारित आकडे आमच्या माहितीसाच्यात जोडत नाही. Algorithm १ संक्षिप्तात तिलसो मुल्यांकनाची प्रक्रिया दाखवतो.

प्रकरण ६

मूल्यमापन

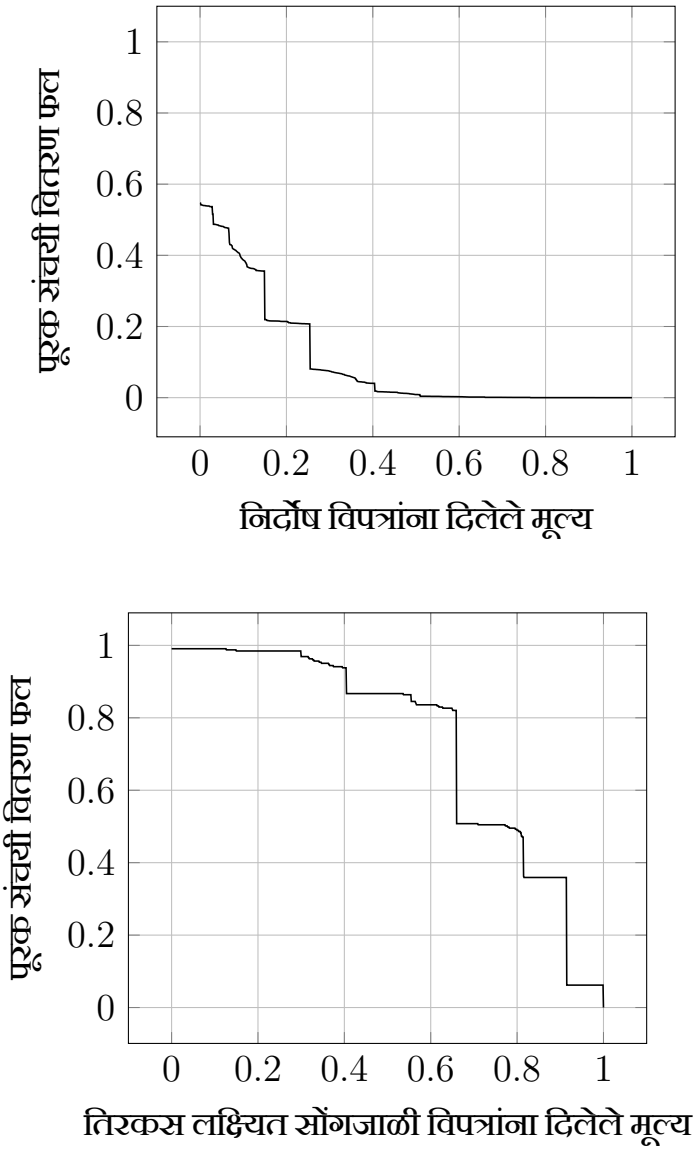
आम्ही आमच्या प्रणालीचे मूल्यमापन सीओईपीतल्या ४० स्वैच्छिकांकडून गोळा केलेल्या ३.५ वर्षां-इतके विपत्रांच्या माहितीसंग्रहाचा वापर करून केले. माहितीसंग्रहात २७ हल्ल्यांचे प्रसंग आहेत जे ३२३ तिरकस लक्ष्यित सोंगजाळी विपत्रांशी सुसंगत आहेत. आमची प्रणाली वापरून, आम्हाला २२ प्रसंग ओळखता आले आणि १ प्रसंग अंशतः ओळखला (हल्ल्यातली काही विपत्रे ओळखली), जे २८० विपत्रांशी सुसंगत आहेत आहेत. याव्यतिरिक्त, २७ पैकी २५ प्रसंग आधी ज्ञात होते व आमची प्रणाली वापरून आम्हाला माहितीसंग्रहातले २ प्रसंग सापडले जे आधी ज्ञात नव्हते. ह्या दोनपैकी एक प्रसंग अत्यंत लक्ष्यित आहे आणि फक्त एका तिरकस लाक्षियत सोंगजाळी विपत्राशी सुसंगत आहे. आम्ही ०.८८% चा चुकीचे-सकारात्मक दर आणि ८६.६९% चा खरे-सकारात्मक दर प्राप्त केले. एकूण अचू-कता ९८.७९% इतकी आहे. विविध कार्यप्रदर्शन मापदंड कोष्टक ६.१ मध्ये दर्शविले आहेत.

चुकीचे-सकारात्मक चे सर्वात सामान्य कारण हे आम्ही वापरात असलेल्या भौगोलिक-आयपी माहि-तीसाच्याने ने सांगितलेल्या चुकीचे शहरे आहे. तपासणी नंतर आम्हाला असे आढळले की प्रेषक प्र-त्यक्षात संस्थेच्या शहरापासूनच विपत्र पाठवत होते, परंतु भौगोलिक-आयपी माहितीसाच्यात आयपी-शहर ह्याचे अयोग्य अनुबंध होते. इतर वैशिष्ट्यांच्या श्रेणींच्या लहान मूल्यांसह ह्या चुकीच्या मुल्यामुळे ति.ल.सो. मूल्य हे ०.५ च्या पुढे गेले. तरीही, कोणत्याही निर्दोष विपत्रांना ०.६५ पेक्षा अधिक मूल्य मिळाले नाही.

आकृती ६.१ दर्शविते की ति.ल.सो. प्रणाली निर्दोष आणि हल्ल्यांच्या विपत्रांना कसे मूल्य देते. ९९.१% निर्दोष विपत्रांना ०.५६% पेक्षा कमी मूल्य मिळाले. तसेच ८६.६% तिरकस लक्ष्यित सोंगजाळी विपत्रांना ०.६५ पेक्षा अधिक मूल्य मिळाले. हे सूचित करते की आमचा संक्षिप्त वैशिष्ट्यांचा संच निर्दोष आणि हल्ल्याच्या विपत्रांना ओळखण्यासाठी पुरेसे अंतर पुरवते.

कोष्टक ६.१: आमच्या मूल्यांकन प्रणालीच्या कामगिरीची विसंगती शोध तंत्रांची तुलना

Algorithm	खरे-सकारात्मक	चुकीचे-नकारात्मक	खरे-नकारात्मक	चुकीचे-सकारात्मक	अचूकता	एफ१ गुण
वि.ल.सी. मूल्यांकन	८६.६१%	१३.३१%	९९.१२%	०.८८%	९८.७९%	७९.३२%
लोकल आउटलायर फॅक्टर	९६.२८%	३.७२%	२.२२%	९७.७८%	४.७४%	५.१४%
एक-वर्ग एसव्हीएम	९९.०७%	०.९३%	४५.३२%	५४.६८%	४६.७६%	९.०७%
ऐवस्ट कोव्हेरियन्स	९१.९५%	८.०५%	९६.३%	३.७%	९६.१८%	५६.३%



आकृती ६.१: ति.ल.सो. मुल्यांकन प्रणाली ने निर्दोष आणि तिरकस लक्ष्यित सोंगजाळी विपत्रांना दिलेल्या मूल्यांचे पूरक संचयी वितरण फल.

६.१ विसंगती शोध पद्धतींसोबत तुलना

आमची आमच्या प्रणालीच्या कामगिरीची तुलना साहित्यातील यंत्र स्वशिक्षणावर आधारित विसंगती शोध तंत्रासोबत करतो [१२, ३१], जे आहेत लोकल आउटलायर फॅक्टर, एक-वर्ग एसव्हीएम, आणि रोबस्ट कोव्हेरीयन्स. प्रत्येक विपत्रासाठी वैशिष्ट्यांच्या वर्गांनी दिलेल्या मूल्यांना सामान्यीकरण करून आम्ही त्यांचे वैशिष्ट्य सदिश तयार करतो. कोष्टक ६.१ मध्ये आम्ही तुलना दर्शविली आहे. जरी एक-वर्ग एसव्हीएम सर्वात जास्त खरे-सकारात्मक दर देतोय, तर त्याचे त्याचा चुकीचे-नकारात्मक चा दर अतिशय अस्वीकार्य आहे. तत्सम परिणाम इतर तंत्रज्ञानात दिसून येतात. अशा प्रकारच्या ह-

ल्यांच्या शोधासाठी सर्व विसंगती शोध तंत्राचा चुकीचे-सकारात्मक दर अव्यवहार्य आहेत. आमचा चुकीचे-सकारात्मक दर, खरे-नकारात्मक दर, अचूकता आणि एफ१ गुण इतर तंत्रांपेक्षा अधिक चांगले आहेत. जरी इतर तंत्रांचे खरे-सकारात्मक दर आणि चुकीचे-नकारात्मक दर आमच्या प्रणालीच्या पेक्षा चांगले आहेत, तरी ते प्रामुख्याने चुकीचे-सकारात्मक दराला कमीकमी ठेवण्याच्या आमच्या प्रयत्नामुळे आहेत. व्यवहार्य असण्यासाठी प्रणालीचा चुकीचे-सकारात्मक दर कमीतकमी असणे अत्यंत महत्वाचे आहे.

मानक विसंगती शोध प्रणाल्या एखादे वैशिष्ट्य मूल्य अधिक असल्याने पूर्ण घटनेला विसंगती निर्धारित करण्याच्या मर्यादेने ग्रस्त आहेत. संस्थेत आढळून आलेल्या निर्दोष वर्तनाच्या विविधतेमुळे, अनेक निर्दोष घटनांचे वेगवेगळ्या वैशिष्ट्यांसाठी विसंगती मुल्ये असू शकतात. आमच्या प्रणालीमध्ये क्षेत्रिय ज्ञान समाविष्ट केल्यामुळे आणि एखाद्या घटनेस एका वैशिष्ट्याच्या उच्च मुल्यामुळे विसंगती ठरवत नसल्याने, ती मानक प्रणालींपेक्षा अधिक चांगले काम करते.

ह्या प्रणाल्या माहिती एका ठराविक वितरणाची असल्याचे गृहीत धरण्याच्या किंवा चांगले निकाल देण्यासाठी प्रशासकाद्वारे मापदंडे साधण्याच्या मर्यादेपासून देखील ग्रस्त असतात. यासारख्या विशेष हल्ल्यांचे वितरण अज्ञात असते आणि संस्थेप्रमाणे बदलू शकते. मापदंडे साधण्यासाठी प्रशासकाद्वारे सूक्ष्म समस्वरण करणे गरजेचे आहे आणि अनुकूल मापदंडे साधण्यासाठी कोणताही स्थापित मार्ग नाही.

प्रकरण ७

चर्चा

आंतरजालीय क्षेत्र हे नेहमीच हल्लेखोरांच्या आणि बचावकर्त्यांच्या रस्सीखेचेच्या स्थितीत असते. या संशोधनाचे आमचे हेतू म्हणजे हल्लेखोरांना तिरकस लक्ष्यित सोंगजाळ्यांचे हल्ले पार पाडण्याला कठीण करणे आहे. आमची प्रणाली अशे हल्ले शोधण्यासाठी संदर्भ-आधारित आणि इतिहास-आधारित वैशिष्ट्ये वापरते. प्रणाली जसजसे अधिक विपत्रांवर प्रक्रिया करते, तसतसे प्रणाली स्वतःला परिष्कृत करत अधिक परिपक्व बनत जाते. ह्याने प्रशासक वास्तविक वेळीमध्ये योग्य कारवाई करू शकतात आणि तडजोड झालेल्या खात्याचा प्रवेश रद्द करून आणखी नुकसान होऊ नये म्हणून हल्ला थांबवू शकतात. मागील प्रकरणात दाखवल्याप्रमाणे आम्हाला संक्षिप्त वैशिष्ट्यांचा संच वापरून उच्च अचूकता मिळवता आली. तसेच, संक्षिप्त वैशिष्ट्यांच्या संचामुळे निर्णय सीमा कमी जटिल आहे. समस्येच्या क्षेत्रावर आधारित, प्रशासक प्रणालीमध्ये आवश्यक वैशिष्ट्ये जोडू शकतात. हे हल्ले अतिविशेष असल्याने त्यांना शोधण्यात क्षेत्रिय ज्ञान मोठ्या प्रमाणावर मदत करू शकते. एखाद्या विपत्राला सोंगजाळी निर्धारित केल्यावर आम्ही डेटाबेस मधल्या इतिहासावर आधारित माहिती अद्यतनित करीत नसल्याने, हल्लेखोर ऐतिहासिकदृष्ट्या तयार केलेल्या पार्श्वरेखांना सहजपणे दुषित करू शकत नाही.

७.१ मर्यादा

प्रणालीची एक स्पष्ट मर्यादा अशी आहे की संस्थेच्या बाहेरच्या विपत्रांच्या पत्त्यांवरून आलेल्या लक्ष्यित सोंगजाळी हल्ल्यांना प्रणाली ओळखू शकत नाही. आमची प्रणाली संस्थेच्या बाहेरून आलेल्या लक्ष्यित सोंगजाळी विपत्रांचा विचार करत नाही नसल्यामुळे, आमची प्रणली अशा विपत्रांकडे दुर्लक्ष करते.

ऐतिहासिक पार्श्वरेखा तयार करण्यासाठी, प्रणालीला पूर्व प्रशिक्षण आवश्यक आहे. मागील प्रकरणात

आम्ही ४ महिन्यांचा प्रशिक्षण कालावधी वापरून सविस्तर निकाल दिले आहेत. आम्ही कमी प्रशिक्षण कालावधीसह देखील प्रणालीची चाचणी केली. या चाचण्यांनी ४ महिन्यांच्या प्रशिक्षण कालावधीच्या तुलनेत जास्तं चुकीचे-सकारात्मक दर दिले. यावरून असे दिसून येते की चांगले परिणाम देण्यासाठी किमान आवश्यक प्रशिक्षण आवश्यक आहे. हा कालावधी वापरकर्त्यांच्या गतिविधीच्या घनतेवर अवलंबून असतो.

विपत्रांच्या मुख्य मजकुरापैकी, आम्ही फक्त विद्यमान दुव्याच्या च्या एफक्यूडीएन ला वापरतो. हा निर्णय मुख्यतः गोपनीयतेच्या कारणामुळे घेण्यात आला. एखादी प्रणाली लिखाणाच्या शैलीचा आणि सामान्य भाषा प्रक्रिया पद्धतींचा वापर करू शकते.

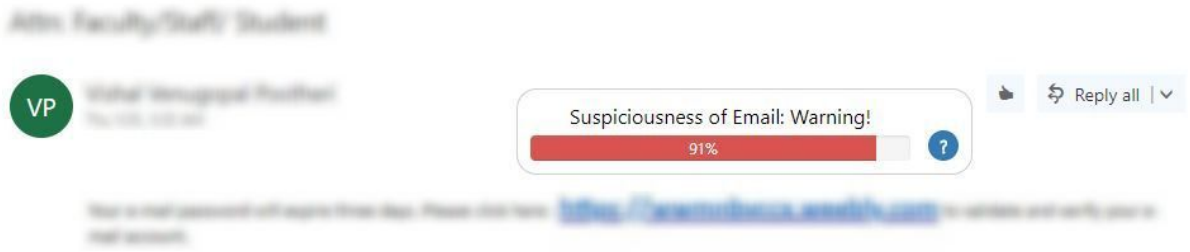
७.१.२ मध्ये स्पष्ट केल्याप्रमाणे, आम्ही प्रवासी वापरकर्ताच्या बाबतीत विचार करत नाही. यामुळे आयपी वैशिष्ट्य श्रेणीतील चुकीच्या मुल्यांची भर पडेल, ज्यामुळे एकूण ति.ल.सो. मूल्यामध्ये बदल होईल आणि अशा प्रकरणांमध्ये चुकीचे वर्गीकरण होऊ शकते.

७.२ ख्रोम एक्सटेन्शन - सीओईपी कुंपण

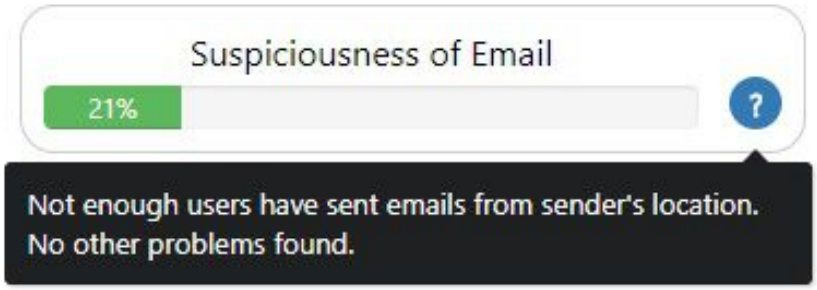
प्रस्तावित प्रणालीचे उद्देश्य प्रामुख्याने विपत्र सेवा प्रदातांद्वारे प्रसंगणकांवर, किंवा संस्थांच्या स्वतःच्या विपत्र प्रसंगणकांवर कार्यान्वित होणे आहे. परंतु, हे नेहमी शक्य नाही. संस्थेच्या आवश्यकतेनुसार, संस्था सर्व आंतर-क्षेत्रिय विपत्रांना प्राप्तकर्त्यांपर्यंत पोहोचण्यास परवानगी देऊन, अंतिम वापरकर्त्याने विपत्राचे काय करावे हे ठरवावे, असा निर्णय घेऊ शकते. किंवा संस्था अशी विपत्र सेवा वापरत असेल ज्यात अश्या प्रकारचे हल्ले ओळखण्याची सोय नसेल. अशा परिस्थितींमध्ये, प्लगईन्स चा वापर करून संस्था आमच्या सारख्या प्रणालीची अंमलबजावणी करू शकते, ज्याने वापरकर्त्यांना विपत्रासंबंधित निर्णय घेण्यास मदत होईल.

आम्ही सीओईपी कुंपण नावाचे ख्रोम एक्सटेन्शन विकसित केले जे आउटलुक वेब वर एक आंतरपृष्ठ घटक दाखवते, जे वापरकर्त्यांना त्यांच्या निर्णयांमध्ये मार्गदर्शन करेल. हे एक्सटेन्शन आम्ही आमच्या ति.ल.सो. प्रणालीला दिलेल्या एपीआय (आज्ञावली आंतरपृष्ठ) चा वापर करते. एक्सटेन्शन हे प्रतिबंधक संरक्षण दृष्टिकोनातून वापरकर्त्यांना चेतावणी संदेश दाखवण्याच्या हेतूने विकसित केले आहे. आंतरपृष्ठाची आखणी ही संबंधित माहितीसह कोपरखळीने टोक्ण्यासारखे करून [५४] वापरकर्त्याचे लक्ष वेधते आणि त्यांना जाणीवपूर्वक निर्णय घेण्यास मदत करते. आकृती ७.१ वापरकर्त्यास दर्शविलेल्या आंतरपृष्ठाच्या घटकांची चित्रे दाखवते. ख्रोम एक्सटेन्शनच्या व्यतिरीक्त, आम्ही सीओईपीमधील प्रशासकांसाठी आमची प्रणाली वापरण्यासाठी आवश्यक असलेली आंतरपृष्ठे विकसित केली आहे, जसे की श्रेणीसोपान तयार करणे आणि आढळलेल्या हल्ल्यांचे तपशील पाहणे. आम्ही सीओई-

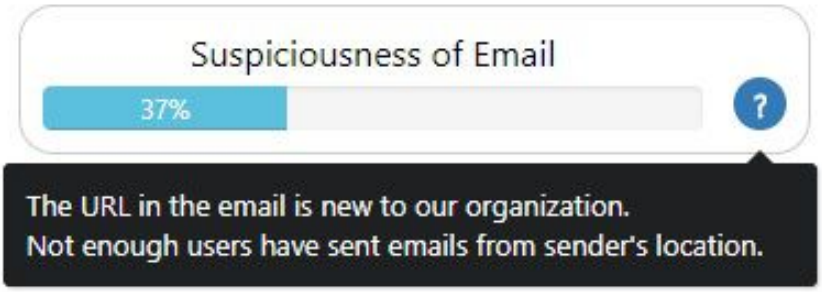
पीच्या बाहेरच्या विपत्र पत्त्यांवरून आलेल्या विपत्रांवर काम करत नाही, म्हणून अशा सर्व विपत्रांसाठी सर्वसामान्य चेतावणी संदेश दर्शवितो आणि अशा विपत्रांसाठी वापरकर्त्यास काळजीपूर्वक पुढे जाण्याची सूचना देतो.



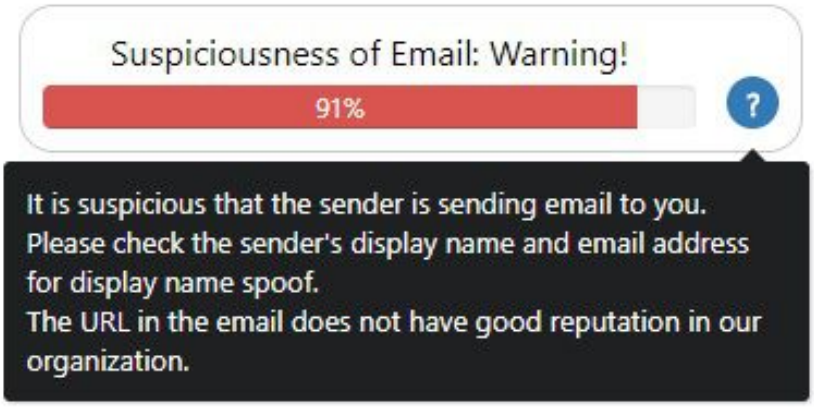
(a)



(b)



(c)



(d)

आकृती ७.१: (a) आउटलुक वेब मधील एका विपत्रामध्ये दाखवलेल्या आंतरपृष्ठ घटकाचे घटकाचे उदाहरण दर्शविते. (b)-(d) आंतरपृष्ठांची संदेशांसहित उदाहरण दर्शवितात, वापरकर्त्याच्या पसंतीवर आधारीत कोपरखळीने टोक्ण्यासारखे किंवा मूषक घुटमळण्याने.

प्रकरण ८

निष्कर्ष

या निबंधात, आम्ही सामाजिक अभियांत्रिकी हल्ल्यांचा एक विशेष वर्ग - तिरकस लक्ष्यित सोंगजाळे - ह्यांचा अभ्यास केला. अश्या हल्ल्यांचा शोध लावणे विशेषतः कठीण आहे कारण ते हल्लेखोरांच्या ताब्यात असलेल्या संस्थेमधील खात्यातून केले जातात. अशी आक्रमणे शोधण्यासाठी एक वास्तविक-वेळी, व्यावहारिक आणि उपयोजित प्रणालीची मांडणी करणे हे आमचे ध्येय होते. आम्ही आमच्या संस्थेतल्या ४० स्वैच्छिकांकडून ३.५ वर्षांइतके विपत्र गोळा केले आणि या खूणचिट्ठी नसलेलेल्या माहिती संग्रहाचे वर्णन सादर केले. आम्ही संस्थेवरील हल्ल्यांच्या आमच्या निरीक्षणावर आधारित विविध वैशिष्ट्य श्रेण्या तयार केल्या. ही वैशिष्ट्ये तिरकस लक्ष्यित सोंगजाळी विपत्रे शोधण्यासाठी आमच्या प्रस्तावित मुल्यांकन प्रणालीला देण्यात आली. आम्ही आमच्या मुल्यांकन प्रणालीचे आमच्या वास्तविक जीवनातील माहिती संग्रहाचा वापर करून मूल्यमापन केले. निकाल दाखवतात की मुल्यांकन प्रणालीने ९८.७९% ची अचूकता आणि ०.८८% चे चुकीचे-सकारात्मक दर प्राप्त केले. तसेच, आम्हाला पूर्वी माहीत नसलेल्या २ हल्ल्यांचे प्रसंग सापडले. आम्ही आमच्या मुल्यांकन प्रणालीच्या कामगिरीची तुलना यंत्र स्वशिक्षण तंत्रज्ञानावर आधारीत विसंगती शोध पद्धतींसोबत केली आणि दाखवले की आमच्या मुल्यांकन प्रणालीने एकंदर अधिक चांगले निकाल दिले. आम्ही सीओईपीतल्या वापरकर्त्यांना अधिक माहितीपूर्ण निर्णय घेण्यास मदत करण्यासाठी ख्रोम एक्सटेन्शन - सीओईपी कुंपण - विकसित केले. असे विशेष हल्ले ओळखण्यासाठी क्षेत्रीय ज्ञान महत्त्वपूर्ण भूमिका बजावू शकते. सध्यःस्थितीत संस्था लक्ष्यित सोंगजाळी हल्ल्यांची बातमी मिळवण्यासाठी वापरकर्त्यांवर अवलंबून असल्याने, हे संशोधन समाधानकारक खरे-सकारात्मक दर व कमीत कमी चुकीचे-सकारात्मक दर ठेवून, तसेच पूर्वी अज्ञात असलेल्या हल्ल्यांच्या प्रसंगांचा शोध लावून सुधारीचे काम करू शकते.

भविष्यातील कार्य. भविष्यातील कार्याचा भाग म्हणून, आम्ही वापरकर्त्यांच्या सर्वेक्षणाद्वारे ख्रोम एक्सटेन्शनचे मूल्यमापन करण्याचे उद्दिष्ट ठेवतो आणि सीओईपीतल्या विविध वापरकर्त्यांच्या निर्णय

घेण्याच्या क्षमतेवर त्याच्या प्रभावाचे मापन करू. आम्ही प्रणालीला सुधारून अधिक चांगले निकाल मिळवण्याकडे व अजून वैशिष्ट्यांना समाविष्ट करण्याकडे देखील पुढे लक्ष देवू. तसेच, माहिती उपलब्ध असल्यास, आम्ही खात्यात प्रवेश करण्यावेळीच्या टप्प्यात हल्लेखोरांना ओळखण्याचे अन्वेषण व मांडणी करून सध्याच्या खात्यात प्रवेश केल्यानंतरच्या घडामोडींवर आधारित मांडणीसोबत एकत्रित करून हल्लेखोरांना ओळखण्याचा प्रयत्न करू शकतो.

संदर्भ सूची

[1] Agari. Agari Global DMARC Adoption Report, 2017.

[2] Syed Mubashir Ali. Integration of information security essential controls into information technology infrastructure library-A proposed framework. *International Journal of Applied Science and Technology*, 4(1), 2014.

[3] A. Almomani, B. B. Gupta, S. Atawneh, A. Meulenberg, and E. Almomani. A Survey of Phishing Email Filtering Techniques. *IEEE Communications Surveys Tutorials*, 15(4) :2070–2090, 2013.

[4] Mohamed Alsharnouby, Furkan Alaca, and Sonia Chiasson. Why phishing still works : User strategies for combating phishing attacks. *International Journal of Human-Computer Studies*, 82 :69–82, October 2015.

[5] Calvin Ardi and John Heidemann. AuntieTuna: Personalized Content-Based Phishing Detection. In *Proceedings of the NDSS Workshop on Usable Security*, San Diego, California, USA, February 2016. The Internet Society.

[6] Zinaida Benenson, Freya Gassmann, and Robert Landwirth. Unpacking Spear Phishing Susceptibility. In *Financial Cryptography and Data Security*, Lecture Notes in Computer Science, pages 610–627. Springer, Cham, April 2017.

[7] Russell Brandom. Two-factor authentication is a mess, July 2017.

[8] Cristian Bravo-Lillo, Saranga Komanduri, Lorrie Faith Cranor, Robert W. Reeder, Manya Sleeper, Julie Downs, and Stuart Schechter. Your Attention Please: Designing Security-decision UIs to Make Genuine Risks Harder to Ignore. In *Proceedings of the Ninth Sympo-*

sium on Usable Privacy and Security, SOUPS '13, pages 6 :1–6 :12, New York, NY, USA, 2013. ACM.

[9] Casey Inez Canfield, Baruch Fischhoff, and Alex Davis. Quantifying Phishing Susceptibility for Detection and Behavior Decisions. *Human Factors*, 58(8) :1158–1172, December 2016.

[10] Ye Cao, Weili Han, and Yueran Le. Anti-phishing Based on Automated Individual White-list. In *Proceedings of the 4th ACM Workshop on Digital Identity Management*, DIM '08, pages 51–60, New York, NY, USA, 2008. ACM.

[11] D. D. Caputo, S. L. Pfleeger, J. D. Freeman, and M. E. Johnson. Going Spear Phishing: Exploring Embedded Training and Awareness. *IEEE Security Privacy*, 12(1) :28–38, January 2014.

[12] Varun Chandola, Arindam Banerjee, and Vipin Kumar. Anomaly detection : A survey. *ACM computing surveys (CSUR)*, 41(3) :15, 2009.

[13] Neil Chou, Robert Ledesma, Yuka Teraguchi, and John C. Mitchell. Client-Side Defense Against Web-Based Identity Theft. In *NDSS*, 2004.

[14] Dan Conway, Ronnie Taib, Mitch Harris, Kun Yu, Shlomo Berkovsky, and Fang Chen. A Qualitative Investigation of Bank Employee Experiences of Information Security and Phishing. In *Thirteenth Symposium on Usable Privacy and Security (${$SOUPS$}$ 2017)*, pages 115–129. USENIX$}$ Association$}$, 2017.

[15] Qian Cui, Guy-Vincent Jourdan, Gregor V. Bochmann, Russell Couturier, and Iosif-Viorel Onut. Tracking Phishing Attacks Over Time. In *Proceedings of the 26th International Conference on World Wide Web*, WWW '17, pages 667–676, Republic and Canton of Geneva, Switzerland, 2017. International World Wide Web Conferences Steering Committee.

[16] Tamara Denning, Adam Lerner, Adam Shostack, and Tadayoshi Kohno. Control-Alt-Hack: The Design and Evaluation of a Card Game for Computer Security Awareness and Education. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, CCS '13, pages 915–928, New York, NY, USA, 2013. ACM.

[17] P. Dewan, A. Kashyap, and P. Kumaraguru. Analyzing social and stylometric features to identify spear phishing emails. In *2014 APWG Symposium on Electronic Crime Research (eCrime)*, pages 1–13, September 2014.

[18] Rachna Dhamija, J. D. Tygar, and Marti Hearst. Why Phishing Works. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '06, pages 581–590, New York, NY, USA, 2006. ACM.

[19] DNSBL. DNSBL, September 2017. Page Version ID : 800548089.

[20] Julie S. Downs, Mandy Holbrook, and Lorrie Faith Cranor. Behavioral Response to Phishing Risk. In *Proceedings of the Anti-phishing Working Groups 2Nd Annual eCrime Researchers Summit*, eCrime '07, pages 37–44, New York, NY, USA, 2007. ACM.

[21] Julie S. Downs, Mandy B. Holbrook, and Lorrie Faith Cranor. Decision Strategies and Susceptibility to Phishing. In *Proceedings of the Second Symposium on Usable Privacy and Security*, SOUPS '06, pages 79–90, New York, NY, USA, 2006. ACM.

[22] S. Duman, K. Kalkan-Cakmakci, M. Egele, W. Robertson, and E. Kirda. EmailProfiler: Spearphishing Filtering with Header and Stylometric Features of Emails. In *2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*, volume 1, pages 408–416, June 2016.

[23] Manuel Egele, Gianluca Stringhini, Christopher Krügel, and Giovanni Vigna. COMPA: Detecting Compromised Accounts on Social Networks. In *NDSS*, 2013.

[24] Serge Egelman, Lorrie Faith Cranor, and Jason Hong. You'Ve Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '08, pages 1065–1074, New York, NY, USA, 2008. ACM.

[25] Adrienne Porter Felt, Robert W. Reeder, Alex Ainslie, Helen Harris, Max Walker, Christopher Thompson, Mustafa Embre Acer, Elisabeth Morant, and Sunny Consolvo. Rethinking Connection Security Indicators. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 1–14, Denver, CO, 2016. USENIX Association.

[26] Jon Fingas. Florida phishing attack exposes data for 30,000 Medicaid recipients, January 2018.

[27] Fireye. Best Defense Against Spear-Phishing Attacks, January 2018.

[28] Edwin Donald Frauenstein and Rossouw von Solms. An Enterprise Anti-phishing Framework. In *Information Assurance and Security Education and Training*, IFIP Advances in Information and Communication Technology, pages 196–203. Springer, Berlin, Heidelberg, July 2009.

[29] David Mandell Freeman, Sakshi Jain, Markus Dürmuth, Battista Biggio, and Giorgio Giacinto. Who Are You? A Statistical Approach to Measuring User Authenticity. In *NDSS*, 2016.

[30] Gerry Gaffney. The myth of the stupid user | Information & Design, 2011.

[31] Markus Goldstein and Seiichi Uchida. A Comparative Evaluation of Unsupervised Anomaly Detection Algorithms for Multivariate Data. *PLOS ONE*, 11(4) :e0152173, April 2016.

[32] B. B. Gupta, Aakanksha Tewari, Ankit Kumar Jain, and Dharma P. Agrawal. Fighting against phishing attacks : state of the art and future challenges. *Neural Computing and Applications*, 28(12) :3629–3654, December 2017.

[33] Mingxing He, Shi-Jinn Horng, Pingzhi Fan, Muhammad Khurram Khan, Ray-Shine Run, Jui-Lin Lai, Rong-Jian Chen, and Adi Sutanto. An Efficient Phishing Webpage Detector. *Expert Syst. Appl.*, 38(10) :12018–12027, September 2011.

[34] Ryan Heartfield and George Loukas. A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks. *ACM Comput. Surv.*, 48(3) :37 :1–37 :39, December 2015.

[35] Grant Ho, Aashish Sharma, Mobin Javed, Vern Paxson, and David Wagner. Detecting Credential Spearphishing in Enterprise Settings. In *26th USENIX Security Symposium (USENIX Security 17)*, pages 469–485, Vancouver, BC, 2017. USENIX Association.

[36] Jason Hong. The State of Phishing Attacks. *Commun. ACM*, 55(1) :74–81, January 2012.

[37] Imperva. Phishing made easy : Time to rethink your prevention strategy ?, December 2016.

[38] Tom N. Jagatic, Nathaniel A. Johnson, Markus Jakobsson, and Filippo Menczer. Social Phishing. *Commun. ACM*, 50(10) :94–100, October 2007.

[39] Ankit Kumar Jain and B. B. Gupta. Phishing Detection: Analysis of Visual Similarity Based Approaches. *Security and Communication Networks*, 2017, 2017.

[40] Mobin Javed. *Detecting Credential Compromise in Enterprise Networks*. PhD thesis, Electrical Engineering and Computer Sciences University of California at Berkeley, December 2016.

[41] M. Khonji, Y. Iraqi, and A. Jones. Mitigation of spear phishing attacks : A Content-based Authorship Identification framework. In *2011 International Conference for Internet Technology and Secured Transactions*, pages 416–421, December 2011.

[42] Brian Krebs. Equifax or Equiphish? — Krebs on Security, September 2017.

[43] Brian Krebs. The Market for Stolen Account Credentials — Krebs on Security, December 2017.

[44] Ponnurangam Kumaraguru. *Phishguru : A System for Educating Users About Semantic Attacks*. PhD thesis, Carnegie Mellon University, Pittsburgh, PA, USA, 2009.

[45] Ponnurangam Kumaraguru, Justin Cranshaw, Alessandro Acquisti, Lorrie Cranor, Jason Hong, Mary Ann Blair, and Theodore Pham. School of Phish: A Real-world Evaluation of Anti-phishing Training. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, SOUPS '09, pages 3 :1–3 :12, New York, NY, USA, 2009. ACM.

[46] Ponnurangam Kumaraguru, Steve Sheng, Alessandro Acquisti, Lorrie Faith Cranor, and Jason Hong. Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology (TOIT)*, 10(2) :7, 2010.

[47] Kaspersky Lab. Phishing for cryptocurrencies : How bitcoins are stolen, January 2018.

[48] Comodo Threat Research Labs. Phishing got Darker and Smarter, January 2018.

[49] Aron Laszka, Jian Lou, and Yevgeniy Vorobeychik. Multi-defender Strategic Filtering Against Spear-phishing Attacks. In *Proceedings of the Thirtieth AAAI Conference on Artificial Intelligence*, AAAI'16, pages 537–543, Phoenix, Arizona, 2016. AAAI Press.

[50] Justin Ma, Lawrence K. Saul, Stefan Savage, and Geoffrey M. Voelker. Beyond Blacklists: Learning to Detect Malicious Web Sites from Suspicious URLs. In *Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, KDD '09, pages 1245–1254, New York, NY, USA, 2009. ACM.

[51] Aaron Mak. Oh Great, a Hacking Group Linked to North Korea Is Getting Very Good at Targeting Bitcoin Owners, February 2018.

[52] Sarah Meyer. Phishing Attacks: Insights from More Than 1,000 Free Phishing Kits - Page 2 of 2, January 2018.

[53] Rob Mueller. SPF, DKIM & DMARC: email anti-spoofing technology history and future, December 2016.

[54] James Nicholson, Lynne Coventry, and Pam Briggs. Can we fight social engineering attacks by social means ? Assessing social salience as a means to improve phish detection. In *Thirteenth Symposium on Usable Privacy and Security (${$SOUPS$}$ 2017)*, pages 285–298. USENIX$}$ Association$}$, 2017.

[55] National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity.

[56] Daniela Oliveira, Harold Rocha, Huizi Yang, Donovan Ellis, Sandeep Dommaraju, Melis Muradoglu, Devon Weir, Adam Soliman, Tian Lin, and Natalie Ebner. Dissecting Spear Phishing Emails for Older vs Young Adults: On the Interplay of Weapons of Influence and Life Domains in Predicting Susceptibility to Phishing. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, CHI '17, pages 6412–6424, New York, NY, USA, 2017. ACM.

[57] Daniela Oliveira, Harold Rocha, Huizi Yang, Donovan Ellis, Sandeep Dommaraju, Melis Muradoglu, Devon Weir, Adam Soliman, Tian Lin, and Natalie Ebner. Dissecting Spear Phishing Emails for Older vs Young Adults: On the Interplay of Weapons of Influence and Life Domains in Predicting Susceptibility to Phishing. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, CHI '17, pages 6412–6424, New York, NY, USA, 2017. ACM.

[58] Exchange Online. Configure your spam filter policies : Exchange Online Protection Help, December 2017.

[59] A. Pecchia, A. Sharma, Z. Kalbarczyk, D. Cotroneo, and R. K. Iyer. Identifying Compromised Users in Shared Computing Infrastructures: A Data-Driven Bayesian Network Approach. In *2011 IEEE 30th International Symposium on Reliable Distributed Systems*, pages 127–136, October 2011.

[60] PhishTank. PhishTank > Frequently Asked Questions (FAQ), 2017.

[61] PhishTank. PhishTank > Friends of PhishTank, 2017.

[62] P. Prakash, M. Kumar, R. R. Kompella, and M. Gupta. PhishNet: Predictive Blacklisting to Detect Phishing Attacks. In *2010 Proceedings IEEE INFOCOM*, pages 1–5, March 2010.

[63] Gowtham Ramesh, Ilango Krishnamurthi, and K. Sampath Sree Kumar. An efficacious method for detecting phishing webpages through target domain identification. *Decision Support Systems*, 61(Supplement C) :12–22, May 2014.

[64] Dylan Sachs. How to Take Down a Phishing Site: 5 Crucial Steps, 2013.

[65] Stuart E. Schechter, Rachna Dhamija, Andy Ozment, and Ian Fischer. The Emperor's New Security Indicators. In *Proceedings of the 2007 IEEE Symposium on Security and Privacy*, SP '07, pages 51–65, Washington, DC, USA, 2007. IEEE Computer Society.

[66] Steve Sheng, Mandy Holbrook, Ponnurangam Kumaraguru, Lorrie Faith Cranor, and Julie Downs. Who Falls for Phish?: A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '10, pages 373–382, New York, NY, USA, 2010. ACM.

[67] Steve Sheng, Brad Wardman, Gary Warner, Lorrie Faith Cranor, Jason Hong, and Chengshan Zhang. An empirical analysis of phishing blacklists. In *Proceedings of Sixth Conference on Email and Anti-Spam (CEAS)*, 2009.

[68] InformationSecurity StackExchange. email - Why does Outlook not block spam sent by employees ? - Information Security Stack Exchange, December 2017.

[69] Steve Sheng, Bryant Magnien, Ponnurangam Kumaraguru, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, and Elizabeth Nunge. Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish. In *Proceedings of the 3rd Symposium on Usable Privacy and Security*, SOUPS '07, pages 88–99, New York, NY, USA, 2007. ACM.

[70] Gianluca Stringhini and Olivier Thonnard. That Ain't You: Blocking Spearphishing Through Behavioral Modelling. In *Detection of Intrusions and Malware, and Vulnerability Assessment*, Lecture Notes in Computer Science, pages 78–97. Springer, Cham, July 2015.

[71] Kurt Thomas, Frank Li, Chris Grier, and Vern Paxson. Consequences of Connectivity: Characterizing Account Hijacking on Twitter. In *ACM Conference on Computer and Communications Security*, 2014.

[72] Arun Vishwanath. Habitual Facebook use and its impact on getting deceived on social media. *Journal of Computer-Mediated Communication*, 20(1) :83–98, 2015.

[73] Jingguo Wang, Yuan Li, and H. Raghav Rao. Overconfidence in Phishing Email Detection. *Journal of the Association for Information Systems*, 17(11), November 2016.

[74] Zikai Alex Wen, Yiming Li, Reid Wade, Jeffrey Huang, and Amy Wang. What.Hack: Learn Phishing Email Defence the Fun Way. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, CHI EA '17, pages 234–237, New York, NY, USA, 2017. ACM.

[75] L. Wenyin, G. Liu, B. Qiu, and X. Quan. Antiphishing through Phishing Target Discovery. *IEEE Internet Computing*, 16(2) :52–61, March 2012.

[76] Colin Whittaker, Brian Ryner, and Marria Nazif. Large-Scale Automatic Classification of Phishing Pages. In *NDSS*, volume 10, page 2010, 2010.

[77] Wikipedia. Google Safe Browsing - Wikipedia, 2017.

[78] Wombat. Email Security or Anti-Phishing Phyllis™ | Wombat Security, 2017.

[79] Min Wu, Robert C. Miller, and Simson L. Garfinkel. Do Security Toolbars Actually Prevent Phishing Attacks? In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '06, pages 601–610, New York, NY, USA, 2006. ACM.

[80] Jing Zhang, R. Berthier, W. Rhee, M. Bailey, P. Pal, F. Jahanian, and W. H. Sanders. Safeguarding academic accounts and resources with the University Credential Abuse Auditing System. In *IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2012)*, pages 1–8, June 2012.

[81] Yue Zhang, Jason I. Hong, and Lorrie F. Cranor. Cantina : A Content-based Approach to Detecting Phishing Web Sites. In *Proceedings of the 16th International Conference on World Wide Web*, WWW '07, pages 639–648, New York, NY, USA, 2007. ACM.

प्रकाशने

1. A. Bhadane, S. Mane, “Detecting Lateral Spear Phishing Attacks in Organizations”, in : *IET Information Security*. Volume No. 13, Issue No. 2, March 2019, p. 133 – 140. ISSN Print : 1751-8709, ISSN Online : 1751-8717, DOI : 10.1049/iet-ifs.2018.5090

2. A. Bhadane, S. Mane, “State of Research on Phishing and Recent Trends of Attacks”, in : *i-manager’s Journal on Computer Science*. Volume No. 5, Issue No. 4, December-February 2018, pp. 14-35, ISSN Print : 2347-2227, ISSN Online : 2347-6141, DOI : 10.26634/jcom.5.4.14608

3. A. Bhadane, S. Mane, “State of Research on User Psychology involved in Phishing Attacks”, in : *Computer Society of India (CSI) Communications*, Volume No. 42, Issue No. 2, May 2018, pp. 34-36,39. ISSN : 0970-647X

4. A. Bhadane, S. Mane, “State of Research on User Training against Phishing with Recent Trends of Attacks”, in : *Centre for Advanced Strategic Studies (CASS) Journal*, April-June 2018, pp.38-53, ISSN 2347-9191