Feltáró jellegű kutatás az egyének biztonsági szokásairól

Bak Gerda

Ph.D. hallgató, Óbudai Egyetem, Biztonságtudományi Doktori Iskola,
bak.gerda@uni-obuda.hu

Dr. Muha Lajos

Egyetemi docens, Nemzeti Közszolgálati Egyetem, Budapest, Magyarország,
muha.lajos@uni-nke.hu

Abstract: Napjainkban a különböző digitális és okoseszközök az életünk szerves részét képezik. A technológiai innovációnak köszönhetően ezek az eszközök folyamatosan fejlődnek, változnak. Nagyban megkönnyítik az életünk, azonban kockázatot is jelentenek, hiszen a különféle okoseszközök internet általi összekapcsolása nem csak nekünk nyújt korlátlan hozzáférhetőséget az adatainkhoz, hanem más, illetéktelen személyeknek is. Az adataink és a magánéletünk védelme azonban nem csak technológiai oldalról igényel védelmet, hanem a felhasználók részéről is. Számos kutatás kimutatta, hogy a védelem leggyengébb pontja az ember. Jelen tanulmányban a felhasználók biztonsági szokásairól kaphatunk képet egy feltáró kutatás keretében. Az eredmények tükrében elmondható, hogy a felhasználók biztonsági szokásai kettősek, egyrészről védik az eszközeiket PIN-kóddal, jelszavakkal, azonban a frissítésekre nem feltétlen figyelnek, mint ahogy a laptopon bekapcsolt Bluetooth-szal sebezhetővé teszik az eszközeiket.

Keywords: IoT, biztonság, biztonsági szokások, mobil, PC

1. Bevezetés

A tárgyak internetének (Internet of Things – IoT) kora megváltoztatta életmódunkat [1]. Bár a tárgyak internete hatalmas előnyöket biztosít, a mindennapi életünkben különböző biztonsági fenyegetéseknek vagyunk kitéve általuk. A biztonsági fenyegetések többsége az információk kiszivárgásával és a szolgáltatások elvesztésével kapcsolatos. A tárgyak internete különböző eszközökből és platformokból áll, különböző hitelesítő adatokkal, ahol minden rendszernek a jellemzőitől függően biztonsági követelményekre van szüksége. A felhasználó magánéletének védelme is a fontos, mivel sok személyes adatot

osztanak meg a különböző típusú eszközök között a felhasználók eszközök között és platformokon [2, 3]. Ezért biztonságos mechanizmusra van szükség a személyes adatok védelméhez.

Jelen tanulmány az emberek digitális eszközeikhez kapcsolódó biztonsági szokásait hivatott feltérképezni, valamint az esetleges kapcsolatokat az egyének szokásai és demográfiai jellemzőik között.

2. Irodalmi áttekintés

Egy 2012-ben készült tanulmány szerint 53 másodpercenként ellopnak egy laptopot; évente pedig 70 millió orosz okostelefon veszik el, és csak 7% -uk kerül meg, továbbá a céges okostelefonok 4,3% -a veszik el / lopják el minden évben [4]. Egy vállalat számára az eszközköltségen kívül a szellemi tulajdon elvesztése és az adatszivárgás is növeli egy-egy mobil elvesztésével járó problémák sorát. Az eszközök védelmére gyakran állítanak be jelszót, azonban a Kaspersky Lab 2015-ös felmérése azt mutatja, hogy az okostelefonok 31% -a és a táblagépek 41% -a nincs jelszóval védve [5], ami szintén növeli az adatlopás kockázatát.

Maga az adatlopás történhet offline vagy online is, a hackerek az interneten, a Bluetooth-on, szöveges üzeneteken vagy a használt online szolgáltatásokon keresztül is eljuthatnak az adatainkhoz. Mivel sokan nincsenek tisztában a modern biztonsági fenyegetésekkel és a működésével, nem fordítanak kellő figyelmet erre. Általánosságban elmondható, hogy az adatokhoz illetéktelenek által történő hozzáférése bekövetkezhet az adott technológia és a felhasználó miatt is.

Ahogy számítógépeink és mobileszközeink több csatlakozási funkciót kapnak, több hely van az adatok átcsúszására. Az új technológiák gyorsabban jönnek létre, mint amennyit meg tudunk védeni. A technológiában rejlő hiányosságra példa az „okos otthonok”, melyek esetén nem rendelkezik az adott eszköz a megfelelő titkostással, amelyek kiskaput kínálnak a hackereknek. A felhasználói hiányosságok pedig a felhasználási szokásokra vezethetők vissza, mint például a nem megfelelő jelszóhasználat, kétes tartalmú emailek megnyitása vagy a jelszavak, azonosítók megosztása harmadik féllel.

A digitális eszközök védelme és sebezhetősége

Az internetre csatlakoztatható eszközök számának növekedése és elterjedése jelentős hatással volt a társadalomra. Ezek, valamint az Internet of Things eszközök az intelligens otthonoktól kezdve a személyes megfigyelőeszközökön át a gyártás automatizálásáig megváltoztatták az életünket, a munkánkat és a szórakozásunkat. Mégis, miközben a felhasználók és az ipar egyaránt széles

körben befogadták az IoT-rendszereket, még nem értettük meg, hogy ezek az eszközök milyen hatással vannak a biztonságunkra [6].

A felhasználók biztonságát és védelmét fenyegető incidensek aggodalmat keltettek a tárgyak internetével kiegészített élet kockázatai miatt, és a technológia használatának korlátozására irányuló lelkes felhívásokhoz vezettek. Ezek a kockázatok korántsem pusztán elméleti jellegűek, olyan következményekkel járhatnak, mint az adatlopás, meghibásodott pacemaker [7] vagy közúti baleset.

A hagyományos biztonsági problémákhoz hasonlóan e hibák nagy része szoftverhibák, felhasználói hibák, rossz konfiguráció és hibás tervezés következménye. Néhány más ok a hibák új osztályát képviseli: a fizikai tereken belüli kölcsönhatások, amelyek nem biztonságos környezethez vezetnek. Az eszközöknek például ellentmondásos céljaik lehetnek: Egy IoT-ajtózár megpróbálhatja bezárni az ajtót, hogy biztosítsa a házat, míg egy füstjelző vészhelyzetben az ajtó feloldásával szeretné biztonságban tudni a lakókat. Ez utóbbi hibák esetén előfordulhat, hogy az egyes eszközök helyesen működnek, de együttesen veszélyes környezetet teremtenek [8].

Az IoT-ben az összes eszköz és ember összekapcsolódik egymással, hogy bármikor és bárhol szolgáltatásokat nyújtson. Az internetre csatlakoztatott eszközök többsége nem rendelkezik hatékony biztonsági mechanizmusokkal, és ki vannak téve különböző adatvédelmi és biztonsági problémáknak, például a titkosítás, az integritás és a hitelesség stb. tekintetében. A tárgyak internete esetében bizonyos biztonsági követelményeknek kell megfelelni, hogy a hálózatot megvédjék a rosszindulatú támadásoktól [9-11]. Azonban hiába a leghatékonyabb védelmirendszer, ha a felhasználó biztonságtudatossági szintje alacsony. Ezért a jelen tanulmány kísérletet tesz a felhasználók biztonságtudatosságának, azon belül is a biztonsági szokásainak feltárására.

3. Módszer

Kutatás célkitűzése

Jelen kutatás egy feltáró jellegű kvalitatív kutatás, amelynek a célja, hogy képet kapjon a digitális eszközök felhasználóinak biztonsági szokásairól, a számítógépekre/laptopokra és a mobiltelefonokra fókuszálva. Ezáltal feltárva és alapot nyújtva egy későbbi, mélyebb és részletesebb kutatáshoz a biztonságtudatosság és a digitális tudás területén.

A kutatás során további célként határozódott meg a lakosság a minél szélesebb körű elérése az online térben generációs vagy egyéb megkötések nélkül, mivel a digitális és okoseszközök mindenki életében jelen vannak és minden korosztályt

érintő kérdésről van szó. Az információbiztonság és a biztonságtudatosság kapcsán több tanulmány is arra az eredményre jutott, hogy a nemek eltérően kezelik a digitális eszközeikett érintő biztonsági kérdéseket [12, 13], továbbá az is kiderült Williams és Ayobami [14] kutatásából, hogy a felhasználók gyakran alábecsülik a kiberfenyegetéseknek való kitettségüket, amely a közösségi média használat során is megjelenik[15]. Ezekhez kapcsolódóan, illetve ezekre alapozva a kutatás elején 2 kutatási kérdés került megfogalmazásra:

K1: Védik-e a digitális eszközeiket a felhasználók?

K2: Van-e különbség a felhasználók digitális eszköz frissítési szokásaiban a nők és férfiak esetében?

Minta és eljárás

Az adatfelvétel 2021.májusában történt, az online kérdőív a LimeSurvey felületen lehetett elérni és a közösségi média felületeken hólabda módszerrel került terjesztésre. A kutatás során alkalmazott kérdőívet 458 fő töltötte ki (342 nő és 116 férfi), az átlagéletkort tekintve a harmincéves korosztály (M = 38,83; SD = 15,224), főként munkavállalók (380 munkavállaló, 78 tanuló) töltötték ki. A legfiatalabb kitöltő 16, míg a legidősebb 76 éves volt. A kitöltőkre vonatkozó részletesebb leíró statisztikai adatokat az 1. táblázat mutatja be. A kérdőív két fő részből tevődött össze, a szocio-demografikus kérdésekből és a digitális eszközökre vonatkozó kérdések részből. A minta nem tekinthető reprezentatívnak.

1.táblázat: A kitöltők leíró statisztikája

		Gyakoriság	Százalék %
Nem	Férfi	116	25,3
	Nő	342	74,7
Kor	<20	8	1,7
	20-34	211	46,1
	35-44	78	17,0
	45-55	79	17,2
	56-64	51	11,1
	65+	31	6,8
Végzettség	kevesebb, mint 8 osztály	0	0
	befejezett 8 osztály	15	3,3
	érettségi	139	30,3
	szakmunkásképző	43	9,4
	főiskolai v. egyetemi diploma	163	35,6
	jelenleg felsőoktatásban tanul	78	17,0
	posztgraduális képzés	16	3,5
	egyéb	4	0,9

4. Kutatási eredmények

A kutatás során összegyűjtött adatok statisztikai elemzése az IBM SPSS Statistics 26 programmal történt.

A kérdőív olyan kérdésekre kereste a választ, mint például, hogy Milyen rendszerességgel csatlakozik a kitöltő a munkahelye által biztosított internetre a saját mobiltelefonjával, illetve a saját laptopjával?, Milyen biztonsági eszközzel gátolja meg, hogy mások is belépjenek a számítógépébe?, Milyen gyakorisággal frissíti a digitális eszközeit, egyáltalán ő végzi-e?.

A digitális eszközök védelme

A következő szekcióban a felhasználók a saját eszközeivel kapcsolatos biztonsági szokásai kerülnek bemutatásra, melyek a következők, munkahelyi internetre való csatlakozás rendszeressége, tűzfal és bluetooth alkalmazása, számítógép/laptop bejelentkezési módok alkalmazása, valamint a digitális eszközök frissítési szokásainak vizsgálata nemek szerinti bontásban.

Ezeket az indokolja, hogy a munkahelyi internet másik fajta védelemmel van ellátva, mint a felhasználók saját, otthoni hálózata, ez pedig lehetőséget nyújt a különféle bizalmas adatok kiszivárogtatására. A sebezhetőséget a különféle védelmi rendszer használata csökkentheti, akárcsak a biztonságos bejelentkezési módok és az operációs rendszerek és alkalmazások rendszeres frissítése, míg a bluetooth folyamatos bekapcsolt állapota csökkenti.

2.táblázat: A kitöltők munkahelyi internetre csatlakozásának gyakorisága

		Gyakoriság	Százalék %
Munkahelyi internetcsatlakozás saját laptoppal	Naponta	127	27,7
	Hetente	24	5,2
	Havonta	29	6,3
	Sosem	278	60,7
Munkahelyi internetcsatlakozás saját mobillal	Naponta	242	52,8
	Hetente	35	7,6
	Havonta	8	1,7
	Sosem	173	37,8

A 2.táblázat foglalja össze, hogy a kitöltők milyen gyakorisággal csatlakoznak az internethez a saját laptojukkal és mobiltelefonjukkal a munkahelyükön. Az eredmények alapján elmondható, hogy a megkérdezett felhasználók nagy része (60,7%) sosem viszi be a munkahelyére a saját laptopját/számítógépét. Azonban a felhasználók kicsit több mint negyede (27,7%) viszont igen, amely azt feltételezi, hogy a munkájához nem kapott számítógépet, vagy a sajátjaként a munkahelyi laptopjára, illetve az egyetemisták is idetartozhatnak. A munkahelyi hálózatra való

csatlakozás nem csak a felhasználó biztonságtudatosságát kérdőjelezi meg, hanem a munkahelye biztonsági irányelveit is.

A táblázat másik felében a mobiltelefonnal történő csatlakozás szerepel. Látható, hogy mobillal a felhasználók 52,8%-a nyilatkozta azt, hogy rendszeresen, napi szinten internetezik ilyen módon. Meglepő módon a megkérdezettek 37,8%-a elmondásuk szerint sosem használja a munkahelye által biztosított internetet a mobiltelefonján. A biztonságtudatosság kapcsán ez is további kérdéseket vet fel. Egyrészt, hogy mi ennek az oka? Másrészt, hogy mennyire tudatos döntés.

3.táblázat: A felhasználók Bluetooth és tűzfal használata

		Gyakoriság	**Százalék %**
Tűzfal	Igen	415	90,6
	Nem	43	9,4
Bluetooth	Igen	120	26,2
	Nem	338	73,8

A 3. táblázat alapján elmondható, hogy a felhasználók jelentős része (90,6%) használja a laptopja/számítógépe egyik alapvető védelmi rendszerét, a tűzfalat. Ezzel szemben a bluetooth bekapcsolt állapota, mely a kitöltők 26,2%-ánál állt fenn, visszás helyzetet eredményez, mivel ezáltal lehetőséget nyújt az esetleges számítógép/laptop hackelésre. Ez felveti a kérdést, hogy a felhasználók tudatában vannak-e a bekapcsolt bluetooth veszélyeinek, illetve hogy ideiglenes, vagy állandó-e a bekapcsolt állapot.

4 táblázat: A felhasználók által alkalmazott bejelentkezési módok laptopon/számítógépen

		Gyakoriság	**Százalék %**
Laptop/PC védelem	PIN-kód	357	77,9
	Jelszó	210	45,9
	Arcfelismerés	216	47,2
	Ujjlenyomat	49	10,7
	Biztonsági kulcs	77	16,8
	Képjelszó	28	6,1
	Egyéb	42	9,2
	Egyik sem	46	10,0

A 4.ábrán került bemutatásra a felhasználók válaszainak megoszlása abban a tekintetben, hogy alkalomaznak-e valamilyen védelemhez kötött bejelentkezési módot, vagy sem. Az erre a kérdésre adott válaszuk alapján a felhasználók biztonsághoz való hozzáállása pozitívnak mondható, hiszen a válaszadók mindössze 10%-a válaszolta, hogy nem használ semmilyen biztonsági bejelentkezési módot sem. Mivel a kérdésre a válaszadás több válasz lehetőségű volt, így a felhasználók több módot is bejelölhettek, ha fennállt ennek az esélye. A

válaszokból az látható, hogy a legnépszerűbb bejelentkezési mód a PIN-kód (357) használata. Ezt követte az arcfelismerés (216) és a jelszó (210).

Frissítési szokások

A következő részben a felhasználók laptop/számítógép és mobiltelefon frissítési szokásai kerülnek bemutatásra aszerint, hogy az említett folyamatot milyen gyakorisággal szokták elvégezni, valamint kereszttábla elemzés keretében elemzésre került, hogy melyik nem minimalizálja a frissítésekkel az eszközeinek sebezhetőségét.

			Milyen gyakran frissíti a saját laptopját/ PC-jét?				**Összes**
			Naponta	Hetente	Havonta	Sosem	
Nem	Férfi	Count	66	21	11	18	116
		% within nem	56,9%	18,1%	9,5%	15,5%	100,0%
		% within frissít	34,7%	21,9%	22,0%	14,8%	25,3%
	Nő	Count	124	75	39	104	342
		% within nem	36,3%	21,9%	11,4%	30,4%	100,0%
		% within frissít	65,3%	78,15	78,0%	85,2%	74,7%
	Összes	Count	190	96	50	122	458
		% of Total	41,5%	21,0%	10,9%	26,6%	100,0%

5 táblázat: A felhasználók laptop/számítógép frissítési szokásai

A 5.táblázatban bemutatott eredmények alapján az egyén saját laptopján/számítógépén elvégzett frissítés gyakorisága és az egyén neme között szignifikáns összefüggés van, mivel $p < 0,05$. Vagyis az, hogy az egyén nő vagy férfi befolyásolja azt, hogy milyen rendszerességgel frissíti a számítógépét. Meg kell azonban jegyezni, hogy a két változó közötti kapcsolat szorosságát mérő Cramer's V együttható érteke 0,193, ami gyenge kapcsolatot jelent. A férfiak nagyobb arányban frissítik az eszközüket naponta (56,9%), mint a nők, akik nem csak 36,3%-a tesz hasonlóan. A nők körében itt is megemlítendő a sosem frissít opció, mely a megkérdezettek 30,4%-ára jellemző, ami sebezhetővé teszi az egyén mobiltelefonját. A férfiak esetében a megkérdezettek mindössze 15,5%- nem frissíti sosem a mobilját.

A naponta frissítést végzők válaszait tekintve felmerülhet a kérdés, hogy vajon mennyire reális a válasz, hiszen egyrészt a számítógépekre érkező frissítések többsége csomagban érkezik a számítógépekre, azaz a felhasználó egy alkalommal nagyobb frissítést hajt végre, valamint néhány napig is eltarthat, de nem naponta történik. Másrészről felvetődik az elmúlt néhány évben tapasztalható Windows frissítési csomagok megbízhatósága, melyek olykor nagyobb kárt okoznak.

			Milyen gyakran frissíti a saját mobilját?				**Összes**
			Naponta	Hetente	Havonta	Sosem	
Nem	Férfi	Count	74	14	15	13	116
		% within nem	63,8%	12,1%	12,9%	11,2%	100,0%
		% within frissít	27,8%	16,3%	45,5%	17,8%	25,3
	Nő	Count	192	72	18	60	342
		% within nem	56,1%	21,1%	5,3%	17,5%	100,0%
		% within frissít	72,2%	83,7%	54,5%	82,2%	74,7%
	Összes	Count	266	86	33	73	458
		% of Total	58,1%	18,8%	7,2%	15,9%	100,0%

6 táblázat: A felhasználók mobiltelefon frissítési szokásai

A 6.táblázatban a mobiltelefonok frissítésének gyakorisága került bemutatásra a nemek viszonylatában. A számítógépekhez hasonlóan ez esetben is összefüggés ($p < 0,05$) mutatkozik a két változó között, melynek az erősségét tekintve a Cramer's V együttható 0,174, vagyis ez esetben is gyenge kapcsolatról van szó. A férfiak részéről az látható, hogy a megkérdezettek több mint fele (63,8%) naponta frissíti a mobiltelefonját, míg a hetente, havonta vagy sosem frissítők aránya közel azonos (12,1-12,9-11,2%). A nőket tekintve a férfiakhoz hasonló eredményeket látni, vagyis a nők több mint fele (56,1%) is naponta frissíti a telefonját, azonban esetükben a ritkább frissítések között nagyobb különbség mutatkozik. Továbbá az is látható, hogy a megkérdezett nők körében 104 fő állítása szerint sosem frissíti a számítógépét, ami növeli a különböző kiberfenyegetéseknek való kitettségét. Ezzel szemben a férfiak részéről hasonlóan minösszesen csak 18 vélekedett.

5. Összegzés

A jelen tanulmány feltáró kutatás révén igyekezett felmérni a felhasználók biztonságtudatosságát, az internetre csatlakozási módok és a digitális eszközök védelmét célzó rendszerek és frissítések alkalmazására fókuszálva. A kutatás két kérdésre kereste a választ, melyek a következők:

Védik-e a digitális eszközeiket a felhasználók? A tanulmányban bemutatott eredmények alapján elmondható, hogy a megkérdezett felhasználók nagy része tesz különféle védelmi intézkedéseket az eszközeinek védelmében, mint például a rendszeres frissítés, a jelszóval, PIN-kóddal történő bejelentkezés, azonban akadnak olyan területek, melyekre kisebb vagy egyáltalán nem fordítanak figyelmet, mint például a bekapcsolt bluetooth vagy a frissítések kihagyása. Így az mondható, hogy a felhasználók biztonságtudatosságán van még mit fejleszteni, azonban mindenképpen érdemes megvizsgálni a mögöttes indítékokat és a magatartást is.

Van-e különbség a felhasználók digitális eszköz frissítési szokásaiban a nők és férfiak esetében? Erre a kérdésre az 5. és 6. táblázat alapján elmondható, hogy igenis van különbség a laptopok és mobilok frissítésének rendszerességének gyakoriságában a nemek tekintetében. A későbbiekben érdemes lehet megvizsgálni a frissítési szokásokat generációnként és akár foglalkozástípus szerint is, valamint mélyebben is megvizsgálni a felhasználók biztonságtudatossági szintjét.

References

[1] I. Hwang, R. Wakefield, S. Kim, and T. Kim, "Security Awareness: The First Step in Information Security Compliance Behavior," Journal of Computer Information Systems, pp. 1-12, 2019.

[2] M. A. Qureshi, A. Aziz, B. Ahmed, A. Khalid, and H. Munir, "Comparative Analysis and Implementation of EfficientDigital Image Watermarking Schemes," *International Journal of Computer and Electrical Engineering,* vol. 4, pp. 558-561, 2012.

[3] M. A. Razzaq, R. A. Sheikh, A. Baig, and A. Ahmad, "Digital Image Security: Fusion of Encryption, Steganography and Watermarking," *(IJACSA) International Journal of Advanced Computer Science and Applications,* vol. 8, pp. 224-228, 2017.

[4] Kensington. (2011). *A Mobile Device is Stolen Every Minute; Most Thieves Strike in the Office or During a Meeting*. Available: https://www.kensington.com/news/news-press-center/2011-news--press-center/a-mobile-device-is-stolen-every-minute-most-thieves-strike-in-the-office-or-during-a-meeting/

[5] Kaspersky. (2015). *A Quarter of Users Don't Understand the Risks of Mobile Cyberthreats, Kaspersky Lab Survey Shows*. Available:

https://www.kaspersky.com/about/press-releases/2015_a-quarter-of-users-don-t-understand-the-risks-of-mobile-cyberthreats-kaspersky-lab-survey-shows

[6] H. F. Atlam and G. B. Wills, "IoT Security, Privacy, Safety and Ethics," pp. 123-149, 2020.

[7] H. Taylor. (2016). *How the 'Internet of Things' could be fatal*. Available: https://www.cnbc.com/2016/03/04/how-the-internet-of-things-could-be-fatal.html

[8] Z. B. Celik, P. McDaniel, G. Tan, L. Babun, and A. S. Uluagac, "Verifying Internet of Things Safety and Security in Physical Spaces," *IEEE Security & Privacy*, vol. 17, pp. 30-37, 2019.

[9] S. Babar, P. Mahalle, A. Stango, N. Prasad, and R. Prasad, "Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT)," in *Recent Trends in Network Security and Applications. CNSA 2010.*, N. Meghanathan, S. Boumerdassi, N. Chaki, and D. Nagamalai, Eds., ed Berlin: Springer, 2010, pp. 420-429.

[10] R. H. Weber, "Internet of Things – New security and privacy challenges," *Computer Law & Security Review*, vol. 26, pp. 23-30, 2010.

[11] L. M. R. Tarouco, L. M. Bertholdo, L. Z. Granville, L. M. R. Arbiza, F. Carbone, M. Marotta, *et al.*, "Internet of Things in healthcare: Interoperatibility and security issues," in *2012 IEEE International Conference on Communications (ICC)*, Canada, 2012, pp. 6121-6125.

[12] Y. J. Park, "Digital Literacy and Privacy Behavior Online," *Communication Research*, vol. 40, pp. 215-236, 2011.

[13] H. Sieger and S. Möller, "Gender differences in the perception of security of mobile phones," in *Proceedings of the 14th international conference on Human-computer interaction with mobile devices and services companion*, ed, 2012, pp. 107-112.

[14] A. Williams and A. S. Ayobami, "Relationship between Information Security Awareness and Information Security Threat," *International Journal of Research in Commerce, IT & Management*, vol. 3, pp. 115-119, 2013.

[15] A. A. Mohamed, O. Ibrahim, and M. Nilashi, "The Security Awareness Framework for Social Network Sites Facebook: Case Study in Universiti Teknologi Malaysia," *Journal of Soft Computing and Decision Support Systems*, vol. 2, pp. 1-8, 2015.