International Journal of Psychosocial Rehabilitation, Vol. 23, Issue 04, 2019
ISSN: 1475-7192

DisCard – Mobile Application for Digitized Contactless Smart Cards Using Near Field Communication

Mohamed Ghaisan Latheef and
Dr. Chandra Reka A/P Ramachandiran

Abstract--- *This paper proposes an online account for storing digitized copies of physical smart cards on the cloud, that are otherwise used for access credentials, subscription to various services, or loyalty programs. Instead of needing to carry around multiple cards for different purposes, or installing multiple separate applications, they can all be accessed by logging into the DisCard application on your chosen mobile device, which will use Near-Field Communication technology in order to emulate the physical card when swiped and scanned. How this application will work is explained, and why the author believes it is better than the currently implemented solution, being physically carrying multiple separate plastic cards with embedded chips. Afterwards, a few papers on related topics are reviewed, with said relation to the application presented, discussed. Results of exploratory surveys indicating viability in the consumer market is analysed and discussed. Positive impacts of switching to digital cards rather than physical ones are then brought to light, such as reduction of plastic waste being beneficial to the environment. Future ideas on improvements as well as limitations of the current application proposed are shown.*

Keywords--- *Contactless Card, Green Computing, Mobile Application, Near Field Communication, Radio Frequency Identification.*

I. INTRODUCTION

Contactless smart cards are prevalent in our current society, whether it be to provide personal identification, cashless payment, loyalty subscriptions, access restrictions for security reasons and many more. Nowadays, the average adult's wallet is weighed down more by the dozens of plastic cards they carry rather than holding paper currency or coins, which has become increasingly sparse in the advent of the modern age.

Research by Markets and Markets© shows that the market for such smart cards will be worth $21.57B by 2023 from $14.22B at 2018, with the Asia Pacific region holding the largest expected share during this period, with companies and governments of developing countries in the region such as Malaysia, India, China and Thailand, using smart cards for authentication and payment. [1]

Smart cards such as the aforementioned, similar to other cards as per the ISO/IEC 7810 ID-1 standard are 85.60mm wide and 53.98mm tall, with a width of 2.88-3.48mm. [2] They use Near Field Communication (NFC), a subset of RFID (Radio-Frequency Identification), which is turn is one of the methods for Automatic Identification and Data Capture (AIDC).

Mohamed Ghaisan Latheef, Asia Pacific University of Technology & Innovation, Bukit Jalil, Kuala Lumpur, Malaysia.
E-mail: TP047492@mail.apu.edu.my
Dr. Chandra Reka A/P Ramachandiran, Asia Pacific University of Technology & Innovation, Bukit Jalil, Kuala Lumpur, Malaysia.
E-mail: chandra.reka@apu.edu.my

Received: 17 Sept 2019 | Revised: 19 Oct 2019 | Accepted: 20 Nov 2019

RFID uses electromagnetic fields to automatically locate and identify tags using radio waves, in which NFC is a subset which utilizes high frequencies, operating at 13.56MHz frequency signal with bandwidth not more than 424Kbit/s, designed for close range secure data exchange. As opposed to older proximity cards which operated at 125kHz, the higher frequency of transmissions allows for substantially more data in less time, letting more data be stored in modern cards. On the other hand, it also means that the range of modern cards are shorter, which is actually advantageous as it decreases the possibility of card skimming or unintended scanning, as the card has to be far closer to the scanner for it to work than was necessary in earlier models.

The same technology is used in mobile phones today, which can allow it to operate in card emulation, reader/writer, and peer-to-peer, occurring between an NFC reader, a passive NFC tag, or another NFC capable device – such as an NFC enabled mobile or tablet – respectively. [3]

II. Materials and Methods

2.1 Previous Studies

2.1.1 Security Vulnerabilities of RFID Card and User Authentication

In the paper by Adeyemi and Bt. Ithnin, they review the vulnerabilities with RFID cards, such as illegal tag cloning, physical damage to the tags, skimming, spoofing, relay, clandestine tracking and many more. [4]

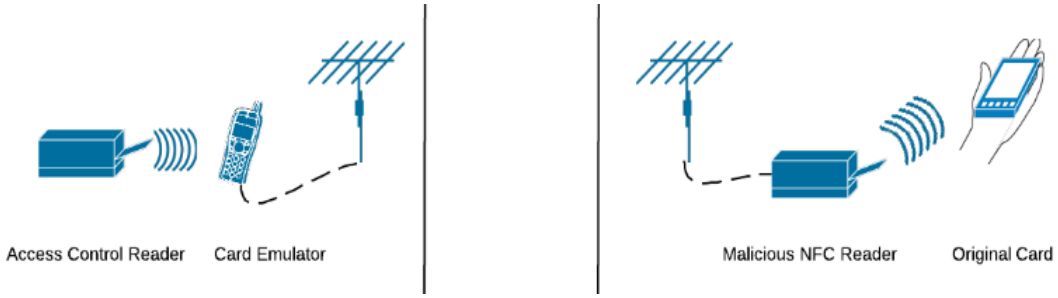

Figure 1: Relay Attack

Skimming, relay and clandestine tracking are both methods used by malicious hackers that take advantage of the promiscuous nature of smart cards, as they do not differentiate between readers, or a specific time or place, and will transmit to any reader as long as it is within range, without the owner even being aware of it.[5] Thus, skimming, where a malicious attacker surreptitiously brings a reader in range of a card in order to make transactions, or illegally copying and cloning the tag via relay is possible. This way, it becomes possible to break into places, impersonate identities, engage in theft, and many other such criminal activities. It can also be used for clandestine tracking, whereby the owner can be tracked by keeping track of the RFID card they are carrying and the signal it gives off, for stalking, kidnapping, burglary or even murder.[6]

The inherent promiscuity also causes interference with scanning cards intentionally as well, such that the card holder would be unable to scan a specific card on a reader as other smart cards they possess in range of the scanner (such as if all of said cards are in a wallet) will also transmit the signal, thereby causing error, therefore having the card holder consciously act to avoid such a scenario by making sure they only have the card they need in range.

Received: 17 Sept 2019 | Revised: 19 Oct 2019 | Accepted: 20 Nov 2019

The other problems of RFID technology, such as man-in-the-middle and denial of service are not as easy to solve, but the solution proposed in this paper would solve the problems highlighted above caused by RFID card promiscuity and constant signal transmission. In a mobile device, NFC features can be turned on when needed, kept off most of the time, and won't even transmit a signal when it is not in emulating card mode. Thus, the timeframe for the attacker to conduct a skimming attack or surveillance is lowered to an infinitesimally small chance, essentially providing a viable solution.

Adeyemi and Bt. Ithnin propose a few of their own solutions as well, one such being a fingerprint authentication on the smart card such that it will only transmit when the user's identity is verified by scanning their fingerprint on the card, both ensuring the identity of the owner and preventing card theft, as well as reducing timeframe of signal transmission only to when needed. Conversely, this would increase the production cost of the card that would be borne by consumers, as well as make it more physically vulnerable to damage and breakage such that any scratches that render the fingerprint scanner non-functioning would essentially mean the card is no longer usable. In the writer's opinion, we already possess a more durable device that we carry around all the time that has necessary biometric sensors or other forms of authentication to verify our identity, that being smartphones. Thus, such a consolidation is not only more effective, but also more efficient. [4]

2.2.2 Environmental Damage caused by Smart Cards

Smart Cards are wasteful and excessive in production, the use of plastic and embedded circuitry therein, as many cards such as personalized cards used for loyalty and credit or debit cards are not reusable and will be destroyed at the end of its usage cycle. Even the cards produced that can be reused in the short term will eventually be rendered obsolete, such as the access cards to a residential building that will eventually age and be demolished, rendering all physical cards defunct. Disregarding that as well, most cards are not durable and fairly flimsy, prone to bending and other such damage.

Figure 2: Plastic Pollution in Ghana

Plastics are chemically made resistant to natural degradation, and is considered a major environmental pollutant, such that even if it wears and tears beyond usability, it merely breaks down into smaller pieces, not base chemical components, and thus retain their composition without composting, making it often toxic to ingest. [7] This has an adverse effect on wildlife habitats, especially marine animals, due to ingestion of plastic waste and exposure to chemicals therein. Thyroid imbalance and carcinogenic effects have also been found in humans.

According to the paper by Finkenzeller, in both 1994 and 1995, around 1 million such smart cards were produced annually for the purpose of public transportation alone, whereas that figure rose quadruple fold on both 1996 and 1997. [8] Not only that, but there is also the carbon dioxide emissions during the production of the card to consider. Investigation by TruCert Ltd on behalf of MasterCard International showed that the average physical polyvinyl chloride (PVC) card has a CO2 footprint of 21 grams, which truly comes up to a massive number when considering the sheer widespread usage and scale. [9] PVC if burnt intentionally or not, releases extremely toxic dioxins, especially noticeable in situations such as landfill fires.

In the article by Géczy et al., biodegradable plastics are proposed as an alternative in the creation of smart cards, for a greener solution as the materials would then naturally compost without any problems. As such, they developed such a prototype using a cellulose-acetate biopolymer based printed circuit board, with a detailed analysis on the manufacturing steps in regard to low cost mass producibility. [10]

In the author's opinion, it is indeed a better solution in terms of what we have now, but making the plastic biodegradable does not eliminate the carbon footprint of its manufacturing. It still requires energy to manufacture, and is not the ideal green solution. Biodegradable polymers still take time to break down, can still be considered a pollutant as it ruins the appearance of coastal areas, and can still be hazardous to swallow for marine life, lack of toxicity notwithstanding.

2.2.3 Multipurpose Smart Cards

Another solution proposed in order to reduce number of smart cards used, possessed and manufactured are multipurpose cards that fulfil various functions, such as access control, electronic wallet, identity verification, and so on.

Malaysia is the first country in the world that has a smart national identity card which has an embedded integrated circuit, including both fingerprint and holder's picture stored inside, as well as other basic information of the cardholder such as gender, address, religion and ethnicity. It can also, as part of the Malaysian Government Multipurpose Card (GMPC) Initiative, serve as a driver's license, public key, electronic purse, health card, an ATM card, as well as other functions. [11][12]

Similarly, Bodake et al. proposes a similar multipurpose national identity card that can be used for voting, train ticketing, and ATM transactions, citing convenience and security.[13]

In fact, such cards are already in widespread usage among universities, where a single card can be used to store money and make cashless transactions in the campus, whether it be at the store, cafeteria, parking, miscellaneous paid services such as printing or paying for bills at the university hostel or accommodations. They can also be used in order to take attendance in classes, queue at counters, as well as ultimately prove they are a student as well, with access to certain parts of the university that may be limited to those studying a particular course.

A paper in 1999 by Welikala et. al. proposes the idea of such a multipurpose smart card in Australian universities, and claims that over a hundred such implementations have already had worldwide success, including in New Zealand, by that point in time. Thus, it can be said this is a fairly old concept, but having a resurgence now

with increased ubiquitous computing and RFID applications, especially in developing countries. [14]

While this does indeed decrease the use of plastic cards by consolidating the function of several into one, it does not eliminate it entirely. Although admittedly, this is better than most smart cards manufactured and used now, with a single purpose.

2.2 Problem Statement

Smart Cards are being increasingly used for various purposes, whether it be for loyalty memberships cards, access control to locations such as private residences or corporate workplaces, as well as for ticketing purposes at toll booths and train stations, as well as other forms of cashless payment. Take for example an average Malaysian middle-class adult living at a rented apartment in a condominium, with a managerial position at a company. They would likely have an access card for the condominium, another card for access to restricted locations at the company, another card for tolls and parking if they drive or to get into the train, around two credit or debit cards, and perhaps one or two loyalty cards for their often frequented retail, restaurant, or another service chain. That's a total of six to seven cards, and this could be hard to keep track of, easily lost, damaged or stolen. Not only such but several of them are necessary in daily usage and thus have to be kept on the person, putting unnecessary burdens on one's pocket.

Their production and disposal causes harm to the environment in terms of plastic pollution, carbon emissions exacerbating global warming, with common materials used in their production breaking down into smaller pieces that are toxic when ingested or inhaled after being incinerated.

They also have vulnerabilities in terms of security, which are especially crucial as some use cases of cards are in payment, and many of which can be solved by the proposed solution.

2.3 Aims and Objectives

This study aims to investigate the feasibility of and propose a mobile application that can store virtual copies of physical smart cards and use the mobile's NFC card emulation feature in order to replicate their use without carrying them around, reducing and eventually aiming to eliminate their usage completely, providing a more secure, cheap and green solution. As such, this application should be able to:

- Create an online account that can act as a secure smart card repository, which can be accessed from any mobile device by logging into the application.
- Read and copy the information stored in a smart card into the online account, such that the mobile phone can be used in lieu of the card with no observable differences.
- Locking application with pin, pattern or biometrics for additional security.
- Enable NFC in phone only when reading, or emulating card, preventing unintended transactions of the card.
- View list of devices connected to the account, including device name, mac address and location. Give option to disconnect a device after additional step to verify identity.

Received: 17 Sept 2019 | Revised: 19 Oct 2019 | Accepted: 20 Nov 2019

2.4 Research Questions

In order to develop the application to both justify a need for it and identify the affected parties, to see whether it is an impactful and a profitable product, the following questions needed to be answered:

- How many smart cards do the average individual carry around on their person daily?
- Identify percentile of individuals that experienced and commonality of smart cards being lost, stolen, broken, skimmed, and/or cloned illegally.
- Degree to which smart card owners that own smartphones – or are willing to buy such devices for new added convenience – would be willing to switch to virtual smart cards.

2.5 Research Methodology

A questionnaire based survey was conducted with both physical questionnaires distributed at random points across the road at different locations, as well as an online one concurrently. This is a form of convenience sampling as it simply looks for the most accessible, taking into account the results of anybody that fills in the online survey or approaches to do the survey on the street. The purpose of this was to ask them how many cards they carry and if they had experienced cards being lost and such (with an optional section to provide details about said incidents), as well as whether they would use an application such as DisCard on their phone to replace their cards. Such a convenience sampling based survey is low in cost in both time and money, since the questions are simple and can be easily answered by anybody fairly quickly as it does not require expert knowledge. The questions asked are also all objective such as quantifiable values, leaving no room for the usual flaws of convenience sampling, which is that groups of friends and relatives may provide answers convenient for the author – that is, as long as the author does not inform them of the purpose behind the questions, and which results are ideal. By itself, the number of cards owned has no right or wrong answer to be interpreted. This allowed for a large fairly unbiased sampling size, to get as widespread a dataset as quickly as possible in the initial stage in order to plan and proceed from there based on the results.

III. RESULTS AND DISCUSSION

3.1 Survey Results

A total of 23 people were questioned on-site as well as 44 online (totalling 67), and they reported the average cards carried to be 3.5, which may have been skewed due to the fact that the location the survey was carried on was at a Malaysian University which uses smartcards as both National Identity cards as well as a card used to access services on University premises. The online survey was also disseminated through using University students and author's colleagues, which meant the respondents were mostly of the same demographic and peer group.

None of the questioned reported any incidents of smart cards being cloned or skimmed, however one did note that their smart card was stolen to secretly access their premises which was protected by RFID access control. 7 reported mild scratches and bends, however only 2 of them noticed any possible degradation in functionality and effectiveness such as range or accuracy. As such, while RFID does have glaring technological security vulnerabilities, evidence suggests that misuse of said vulnerabilities for maligned purposes are not commonplace, at

Received: 17 Sept 2019 | Revised: 19 Oct 2019 | Accepted: 20 Nov 2019

least not yet, whether it is due to the stalwart efforts of local law enforcement or the average criminal lacking the knowhow. Rather, accidental physical damage to the flimsy cards remain the relatively larger issue. However, the possibility still remains, and it is likely that the respondents perhaps are simply not lucrative enough targets for criminals sophisticated enough in terms of knowledge and technology to attempt such a heist.

As far as 45 of the respondents claim to have left behind or lost (temporarily or permanently) a smart card somewhere at some point in their lives, with as many as 39 amongst them claiming this caused them undue distress as the cards were important, not merely loyalty cards and such. On the other hand, the follow up question of whether how many of the respondents left behind or lost (temporarily or permanently) their smartphones, only 14 claimed to have done so, likely as it was simply something they paid more attention to and thus had more awareness of in their day-to-day life.

All of the respondents owned smartphones with the minimum capabilities required of the proposed application, and an overwhelming 61 of 67 agreed the idea was promising and to at least use it on a trial basis. This may, once more, be skewed as the demographic in question is rather tech-savvy, whereas it may not be so well received by the older populace, which the survey unfortunately did not take into account as much.

3.2 Proposed Solution

The DisCard application will allow all users of smart cards to essentially discard them, using emulated versions on their mobile phones instead. This will in turn be more secure, convenient to carry, and easier to share as well as access. This will also benefit the environment as future developments will completely be rid of card cloning altogether and merely cards existing and issued in virtual space, leading to a reduction of plastic manufacturing which means there is less plastic pollution but also less carbon dioxide emissions to the atmosphere, thus reducing the anthropological effect on global warming.

The application requires an android or iOS smartphone with NFC connectivity, so that it can be installed and used.

Upon installation, the user will be prompted to register or login if they already have an account, which will then link the device to the digital cards associated with that account stored remotely on a server.

On logging in, the application will synchronize with the server data, downloading the card information into the mobile storage so that the card emulation functions can be used offline. This is less secure but important as some use cases of smart cards involve locations such as underground railway stations where the mobile might not have cellular range.

After initial registration, user will be briefed on how to read in a smart card, as well as prompted on setting a security feature for successive accessing attempts, whether it be pin, password, pattern, or biometrics such as fingerprints or face.

The application uses push-based messaging so that any new cards added to the account will automatically be synced with all the client devices associated with that account. Thus, a parent can let his/her children log into his/her DisCard account in their own devices in order to use payment cards and such, but also disconnect any of their

devices just as easily by being able to view connected devices using the application. This works even in the case of the device being stolen, as the actual owner of the account can log in from a different platform and disconnect the stolen device from the account.

When cards are successfully synced with the device from the server or newly added through reading a physical card, it can then be emulated in place of the actual card. When the card is to be used, the application can be opened, and the card to emulate selected. For security purposes, the selection will enable NFC to emulate the card for 10 seconds (a duration that can be adjusted or disabled if the user wishes), before it automatically turns back off, preventing it from being skimmed or read unintentionally.

Figure 3: Mobile Payment with NFC

The application has a recurring fee as the costs to maintain the servers and databases storing the account data, as well as the infrastructure to communicate seamlessly with multiple devices, a dedicated team for penetration testing and security due to the sensitive nature of the data, in order to prevent payment cards from being used by hackers. It would also not only require bug fixing, but iterative improvements based on new technology based on new devices, improving functionality and graphical user interface (GUI). Thus, in order to cover the costs as well as keep a profit, the device can serve advertisements in the form of banners to users, with a premium subscription option to remove the advertisements (freemium). The free account features can also be limited to two or three devices, and limited number of cards, with a subscription to store more cards and log into more devices at once.

3.2.1Limitations and Future Improvements

As opposed to physical smart cards, smartphones can run out of charge, after which it would no longer be able to emulate cards. Conversely, this is not that much of a concern as, phones being as pervasive in daily life as it is now, it is rare and unexpected to reach such a situation, with no way to circumvent it, whether it be a portable charger or power bank.

Secondly, instead of replicating multiple physical cards after purchasing them, this is still in fact not an effective solution in terms of environmental conservatism and efficiency on all other observable metrics, as one would first need to possess the manufactured plastic card and replicate it before using it. This application is still a temporary Band-Aid and not a true permanent cure, as it relies on the premise of there being a physical card, thereby this

solution at its current stage cannot get rid of smart cards permanently. Instead, if in the future DisCard can directly link up with companies as a platform similar to Amazon or Grab, where end-users can be both companies or other organizations that issue virtual cards as well as owners and users of said cards. It can allow for businesses and gated communities and such to temporarily issue a virtual card which will be stored in the consumer's account, and revoke said permissions later. This would especially work in places such as condominiums, where people not returning their smart access card upon vacating the premises can later than use the card if the office forgot to cancel it. With the application, card permissions can be made to expire, and this could be applied to any entrance, whether it even be road tolls or getting an entry into the club for a single night only, or gym memberships with monthly renewal.

IV. CONCLUSION

Whilst not necessarily the optimum solution yet, DisCard is a way forward in order to reduce usage of plastic contactless smart cards, which not only have countless security vulnerabilities, being scanned by any scanner in range, and are also easily damaged, lost or stolen. They are also harmful to the environment – its production and continued existence without breaking down, as well as the toxic fumes released when burned by most of the materials used in making such cards. By using NFC technology embedded in mobile phones to emulate card functionality, hopefully it is a step forward to completely get rid of plastic smart card usage altogether, as their continued usage is not a very smart decision.

While DisCard in its current iteration is a stopgap measure, its future iterations as highlighted in section 9 has potential in the author’s opinion to completely replace the smart card industry, taking over the current market of existing users.

REFERENCES

[1] MarketsandMarkets, “Smart Card Market worth 21.57 billion USD by 2023,” 1 June 2018. [Online]. Available: https://www.marketsandmarkets.com/PressReleases/smart-card-market.asp. [Accessed 26 April 2019].

[2] International Organization for Standardization, “ISO/IEC 7810:2003 - Identification cards -- Physical characteristics,” 2003. [Online]. Available: https://www.iso.org/standard/31432.html. [Accessed 26 April 2019].

[3] B. Ozdenizci, M. Alsadi, K. Ok and V. Coskun, “Classification of NFC Applications in Diverse Service Domains,” *International Journal of Computer and Communication Engineering*, vol. 2, no. 5, pp. 614-620, 2013.

[4] I.R. Adeyemi and N. Bt. Ithnin, Users Authentication and Privacy control of RFID Card, 1 ed., Kuala Lumpur: Universiti Teknologi Malaysia, 2012.

[5] T. Haver, Security and Privacy in RFID Applications, 1 ed., Trondheim: Norwegian University of Science and Technology, 2006.

[6] J.K. Marci Meingast, “Security and Privacy,” Journal Of Communications, vol. 2, no. 7, pp. 36-48, 2007.

[7] C. Le Guern, “When The Mermaids Cry: The Great Plastic Tide,” Coastal Care, 1 March 2018.

[8] K. Finkenzeller, RFID Handbook: Fundamentals And Applications In Contactless Smart Cards, Radio Frequency Identification And Near Field Communication, 1st ed., Chichester, West Sussex: *John Wiley & Sons*, Ltd, 2010.

[9] TruCert Ltd, “Carbon Footprint of the Card Industry,” 20 June 2012. [Online]. Available: http://www.icma.com/ArticleArchives/CarbonFootprint_SE2-12.pdf. [Accessed 29 April 2019].

[10] A. Géczy, G. Horváth, L. Dudás, L. Gál, I. Hajdu and G. Harsányi, “RFID cards on biodegradable substrates - Realization aspects and future trends,” 2015 38th *International Spring Seminar on Electronics Technology (ISSE)*, vol. 1, no. 1, pp. 52-56, 2014.

Received: 17 Sept 2019 | Revised: 19 Oct 2019 | Accepted: 20 Nov 2019

[11] The Star Online, "One card for all," 1 February 2010. [Online]. Available: https://www.thestar.com.my/lifestyle/features/2010/02/01/one-card-for-all/. [Accessed 26 April 2019].

[12] P.H. Yeow, W.H. Loo and S.C. Chong, "Accepting Multipurpose "Smart" Identity Cards in a Developing Country," *Journal of Urban Technology*, vol. 14, no. 1, pp. 23-50, 2007.

[13] A. Bodake, V. Baviskar, A. Bodake, S. Bhoite and N. J. Kulkarni, "Multipurpose Smartcard System," *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, vol. 1, no. 9, pp. 175-178, 2012.

[14] J. Welikala, D. Fowler and P. Swatman, Introducing Multi-purpose, Multi-function Smart Cards to Australian Universities, Melbourne, Australia: Monash University, 1999.

[15] P. Mary Jeyanthi, Santosh Shrivastava Kumar "The Determinant Parameters of Knowledge Transfer among Academicians in Colleges of Chennai Region", *Theoretical Economics Letters*, 2019, 9, 752-760, ISSN Online: 2162-2086, DOI: 10.4236/tel.2019.94049, which is in B category of ABDC. List. https://www.scirp.org/journal/Home.aspx?IssueID=12251

[16] P. Mary Jeyanthi, "An Empirical Study of Fraudulent and Bankruptcy in Indian Banking Sectors", *The Empirical Economics Letters*, Vol.18; No. 3, March 2019, ISSN: 1681-8997, which is in C category of ABDC List. http://www.eel.my100megs.com/volume-18-number-3.htm

[17] Mary Jeyanthi, S and Karnan, M.: "Business Intelligence: Hybrid Metaheuristic techniques", *International Journal of Business Intelligence Research*, - Volume 5, Issue 1, April-2014. URL: Https://Dl.Acm.Org/Citation.Cfm?Id=2628938; DOI: 10.4018/ijbir.2014010105, which is in C category of ABDC List.

[18] P. Mary Jeyanthi, "Industry 4.O: The combination of the Internet of Things (IoT) and the Internet of People (IoP)", *Journal of Contemporary Research in Management*, Vol.13; No. 4 Oct-Dec, 2018, ISSN: 0973-9785.

[19] P. Mary Jeyanthi, "The transformation of Social media information systems leads to Global business: An Empirical Survey", *International Journal of Technology and Science (IJTS)*, issue 3, volume 5, ISSN Online: 2350-1111 (Online). URL: http://www.i3cpublications.org/M-IJTS-061801.pdf

[20] P. Mary Jeyanthi," An Empirical Study of Fraud Control Techniques using Business Intelligence in Financial Institutions", *Vivekananda Journal of Research* Vol. 7, Special Issue 1, May 2018, ISSN 2319-8702(Print), ISSN 2456-7574(Online). URL: http://vips.edu/wp-content/uploads/2016/09/Special-Issue-VJR-conference-2018.pdf Page no: 159-164.

[21] Mary Jeyanthi, S and Karnan, M.: "Business Intelligence: Artificial bear Optimization Approach", *International Journal of Scientific & Engineering Research*, Volume 4, Issue 8, August-2013. URL: https://www.ijser.org/onlineResearchPaperViewer.aspx?Business-Intelligence-Artificial-Bear-Optimization-Ap-proach.pdf

[22] Mary Jeyanthi, S and Karnan, M.: "Business Intelligence: Optimization techniques for Decision Making", *International Journal of Engineering Research and Technology*, Volume 2, Issue 8, August-2013. URL: https://www.ijert.org/browse/volume-2-2013/august-2013-edition?start=140

[23] Mary Jeyanthi, S and Karnan, M.: "A New Implementation of Mathematical Models with metaheuristic Algorithms for Business Intelligence", *International Journal of Advanced Research in Computer and Communication Engineering*, Volume 3, Issue 3, March-2014. URL: https://ijarcce.com/wp-content/uploads/2012/03/IJARCCE7F-a-mary-prem-A-NEW-IMPLEMENTATION.pdf

[24] Dr. Mary Jeyanthi: "Partial Image Retrieval Systems in Luminance and Color Invariants: An Empirical Study", *International Journal of Web Technology* (ISSN: 2278-2389) – Volume-4, Issue-2. URL: http://www.hindex.org/2015/p1258.pdf

[25] Dr. Mary Jeyanthi: "CipherText Policy attribute-based Encryption for Patients Health Information in Cloud Platform", *Journal of Information Science and Engineering* (ISSN: 1016-2364)

[26] Mary Jeyanthi, P, Adarsh Sharma, Purva Verma: "Sustainability of the business and employment generation in the field of UPVC widows" (ICSMS2019).

[27] Mary Jeyanthi, P: "An Empirical Survey of Sustainability in Social Media and Information Systems across emerging countries", *International Conference on Sustainability Management and Strategy"* (ICSMS2018).

[28] Mary Jeyanthi, P: "Agile Analytics in Business Decision Making: An Empirical Study", *International Conference on Business Management and Information Systems"* (ICBMIS2015).

[29] Mary Jeyanthi, S and Karnan, M.: "Business Intelligence – soft computing Techniques", *International Conference on Mathematics in Engineering & Business Management* (ICMEB 2012).

[30] Mary Jeyanthi, S and Karnan, M.: "A Comparative Study of Genetic algorithm and Artificial Bear Optimization algorithm in Business Intelligence", *International Conference on Mathematics in Engineering & Business Management* (ICMEB 2012).

[31] Mary Jeyanthi, S and Karnan, M.: "Business Intelligence: Data Mining and Optimization for Decision Making", 2011 *IEEE International Conference on Computational Intelligence and Computing Research* (2011 IEEE ICCIC).

[32] Mary Jeyanthi, S and Karnan, M.: "Business Intelligence: Data Mining and Decision making to overcome the Financial Risk", 2011 IEEE International Conference on Computational Intelligence and Computing Research (2011 IEEE ICCIC).

[33] Dr. Mary Jeyanthi, S: "Pervasive Computing in Business Intelligence", State level seminar on Computing and Communication Technologies. (SCCT-2015)

[34] Dr.P. Mary Jeyanthi, "Artificial Bear Optimization (ABO) – A new approach of Metaheuristic algorithm for Business Intelligence", ISBN no: 978-93-87862-65-4, Bonfring Publication. Issue Date: 01-Apr-2019

[35] Dr.P.Mary Jeyanthi, "Customer Value Management (CVM) – Thinking Inside the box" – ISBN: 978-93-87862-94-4, Bonfring Publication, Issue Date: 16-Oct-2019.

[36] Jeyanthi, P.M., & Shrivastava, S.K. (2019). The Determinant Parameters of Knowledge Transfer among Academicians in Colleges of Chennai Region. Theoretical Economics Letters, 9(4), 752-760.

Received: 17 Sept 2019 | Revised: 19 Oct 2019 | Accepted: 20 Nov 2019