Pricing Data Tampering in Automated Fare Collection

[1]R.Sudhakar, [2]D.Pavithra, [3]S.Reshma Supriya, [4]M.Thenmozhi, [5]R.Vinothini

[1]Assistant Professor, [2,3,4,5]UG Students – Final Year,
Department of Computer Science and Engineering,
Nandha College of Technology, Perundurai, Tamilnadu, India

***Abstract*: Mechanized Fare Collection (AFC) frameworks have been around the world sent for quite a long time, especially in the public transportation network where the travel charge is determined dependent on the length of the outing (a.k.a., distance-based evaluating AFC frameworks). Albeit most messages of AFC frameworks are unreliably moved in plaintext, framework administrators didn't give a lot of consideration to this weakness, since the AFC network is essentially secluded from the public organization (e.g., the Internet) — it is highly unlikely of misusing such a weakness from an external perspective of the AFC organization. In any case, as of late, the appearance of Near Field Communication (NFC)- prepared advanced cells has opened up a channel to attack into the AFC network from the portable Internet, i.e., by Host-based Card Emulation (HCE) over NFC-prepared PDAs. In this paper, we distinguish a novel worldview of assaults, called Less Pay against current distance-based valuing AFC frameworks, empowering clients to pay considerably less than what they should be charged. The distinguished assault has two significant properties: 1) it is imperceptible to AFC framework administrators in light of the fact that the assault never causes any irregularity in the back-end information base of the administrators; and 2) it very well may be adaptable to influence countless clients (e.g., 10,000) by just requiring a moderate-sized AFC card pool (e.g., containing 150 cards). To assess the viability of the assault, we built up a HCE application to dispatch the LessPay assault; and this present reality tests show not just the practicality of the LessPay assault (with 97.6% achievement rate) yet in addition its minimal effort as far as transmission capacity and calculation. At last, we propose, execute and assess four sorts of countermeasures, and present security investigation and correlation of these countermeasures on protecting against the LessPay assault.**

1. Introduction

Mechanized Fare Collection (AFC) systems have been around the globe passed on for a significant long an ideal opportunity to robotize manual labelling and charging structures, particularly in open transportation associations. As movement courses in present day metropolitan territories are by and large extremely long, most of the present AFC systems get a partition based esteeming approach, where the movement charge is resolved subject to the length of the journey. Up to this point, billions of AFC cards have been given ludicrous. A typical AFC structure utilize a symmetric encryption system (e.g., considering 3DES or AES count) to affirm both the components and messages included.

Exactly when an AFC card is legitimately given, an unchangeable unique trade key, TK, is created into the card, which will be used to deliver a powerful gathering key, SK; and a message approval code (or Macintosh) during the charge stage. Amazingly, the wide scope of different data (e.g., the way or leave information used for calculating the excursion cost) exchanged between AFC cards and terminals

2. Automated Fare Collection

A mechanized charge assortment (AFC) framework is the assortment of segments that robotize the tagging arrangement of a public transportation organization - a computerized rendition of manual passage assortment. An AFC framework is generally the reason for coordinated tagging. Ticket office terminals - where a media holder can buy an option to go from staff in an office, or enquire concerning the worth and travel rights related with the media General tagging machines at the Expo station in Singapore, where suburbanites can enhance their EZ-Link card or buy a solitary outing ticket. Ticket candy machines - where a media holder can buy an option to go from a self-administration machine, or enquire regarding the worth and travel rights related with the media Fare door - frequently utilized in a train station so a media holder can access a paid territory where travel administrations are given Stand-alone validator - used to affirm that the media holds a fitting travel right, and to compose the use of the media onto the media for later check (for example by a conductor/assessor). Frequently utilized in verification of- instalment frameworks. On-vehicle validator - utilized by a media holder to affirm travel rights and board a vehicle (for example transport, cable car, train) Inspector/conductor gadget - utilized by staff, for example, a conductor to check travel rights Unattended gadgets are frequently called "validators", a term which began with gadgets that would stamp a date/time onto paper passes to give evidence of legitimate instalment to a conductor.

3. Near Field Communication

Close Field-Communication (NFC) is a bunch of correspondence conventions for correspondence between two electronic gadgets over a distance of 4 cm (11⁄2 in) or less. NFC offers a low-speed association with straightforward arrangement that can be utilized to bootstrap more-proficient remote connections. NFC gadgets can go about as electronic character archives and key cards. They are utilized in contactless instalment frameworks and permit versatile instalment supplanting or enhancing frameworks, for example, Master card and electronic ticket keen cards. This is some of the time called NFC/CTLS or CTLS NFC, with contactless truncated CTLS. NFC can be utilized for sharing little documents like contacts, and bootstrapping quick associations with share bigger media, for example, photographs, recordings, and different documents

4. Host-Based Card Emulation

Host card imitating (HCE) is the product engineering that gives precise virtual portrayal of different electronic personality (access, travel and banking) cards utilizing just programming.

Preceding the HCE engineering, close to handle correspondence (NFC) exchanges were chiefly done utilizing secure components. HCE empowers portable applications running on upheld working frameworks to offer instalment card and access card arrangements autonomously of outsiders while utilizing cryptographic cycles customarily utilized by equipment based secure components without the requirement for an actual secure component. This innovation empowers the dealers to offer instalment cards arrangements all the more effectively through versatile shut circle contactless instalment arrangements, offers ongoing dissemination of instalment cards and takes into account a simple sending situation that doesn't expect changes to the product inside instalment terminals.

5. Triple DES

In cryptography, Triple DES (3DES or TDES), formally the Triple Data Encryption Algorithm (TDEA or Triple DEA), is a symmetric-key square code, which applies the DES figure calculation multiple times to every information block. The Data Encryption Standard's (DES) 56-bit key is not, at this point thought about satisfactory notwithstanding present day cryptanalytic methods and supercomputing power. Be that as it may, an adjusted rendition of DES, Triple DES (3DES), utilizes a similar calculation to deliver a safer encryption. While the public authority and industry norms curtail the calculation's name as TDES (Triple DES) and TDEA (Triple Data Encryption Algorithm), RFC 1851 alluded to it as 3DES from the time it originally proclaimed the thought, and this namesake has since come into wide use by most sellers, clients, and cryptographers. Similarly as with all square codes, encryption and unscrambling of different squares of information might be performed utilizing an assortment of methods of activity, which can for the most part be characterized freely of the square code calculation. Notwithstanding, ANS X9.52 determines straightforwardly, and NIST SP 800-67 indicates by means of SP 800-38A that a few modes will just be utilized with specific requirements on them that don't really apply to general determinations of those modes. For instance, ANS X9.52 determines that for figure block binding, the introduction vector will be diverse each time, while ISO/IEC 10116 doesn't. FIPS PUB 46-3 and ISO/IEC 18033-3 characterize just the single square calculation, and don't put any limitations on the methods of activity for different squares.

6. Security

By and large, triple des with three autonomous keys (keying choice 1) has a critical length of 168 pieces (three 56-bit des keys), yet because of the compromise assault, the successful security it gives is just 112 pieces. Keying choice 2 decreases the powerful key size to 112 pieces (in light of the fact that the third key is equivalent to the first). Notwithstanding, this alternative is powerless to certain picked plaintext or known-plaintext assaults, and subsequently it is assigned by to have just 80 pieces of safety. This can be viewed as unreliable, and, as result triple des has been censured by in 2017.logo of the sweet32 assault the short square size of 64 pieces makes 3des defenceless against block crash assaults on the off chance that it is utilized to scramble a lot of information with a similar key.

7. Related Work

Fan Dang, Pengfei Zhou et al., has proposed in this paperAutomated Fare Collection (AFC) frameworks have been universally sent for quite a long time, especially in open transportation. Albeit the exchange messages of AFC frameworks are for the most part moved in plaintext, which is clearly shaky, framework administrators don't have to give a lot of consideration to this issue, since the AFC network is all around disconnected from public organization (e.g., the Internet). In any case, lately, the approach of Near Field Communication (NFC)- prepared cell phones has overcome any barrier between the AFC organization and the Internet through Host-based Card Emulation (HCE). Spurred by this reality, we plan and practice a novel worldview of assault on present day distance-based valuing AFC frameworks, empowering clients to pay substantially less than really required. [1]. Chris J. Mitchell et al., has proposed in this paper revaluates the security offered by 2-key triple DES, an encryption strategy that remains generally utilized in spite of as of late being de-normalized by NIST. A speculation of the 1990 van Oorschot-Wiener assault is portrayed, comprising the main development in cryptanalysis of 2-key triple DES since 1990. We give further assault upgrades that together infer that the broadly utilized gauge that 2-key triple DES gives 80 pieces of safety can presently don't be viewed as traditionalist; the generally expressed attestation that the plan is secure as long as the key is changed routinely is likewise tested. The primary end is that, while not totally broken, the edge of wellbeing for 2-key triple DES is thin, and endeavours to supplant it, in any event with its 3-key variation, and ideally with a more present day code like AES, ought to be sought after with some criticalness. The way that the van Oorschot-Wiener assault works with both plaintext/ciphertext sets created utilizing a variety of keys and with part of the way known plaintext essentially develops the arrangement of situations wherein the security of 2-key triple DES is in danger. [2]. Ryan Erenhouse et al., has proposed in this paper For some individuals, paying with a card is as yet connected with a "swipe" or a "plunge"; in any case, for the proprietors of in excess of 370 million contactless cards acknowledged in more than 8 million areas in 111 nations, they pay with a tap. Mastercard previously presented contactless cards back in 2003 to give purchasers a protected and basic approach to pay that helps speed them through the checkout line. Furthermore, that equivalent primary innovation (and a significant number of similar principles) likewise controls our capacity to pay with a telephone. Contactless innovation was created by Mastercard with the outlook of never forfeiting security for comfort. The cards and gadgets contain an implanted chip and a radio recurrence (RFID) reception apparatus that give a remote connection the contactless peruser. [3]. WeixiGu,LongfeiShangguan,Zheng Yang et al., has proposed in this paperSleep quality assumes an essential part in close to home wellbeing. A lot of exertion has been paid to configuration rest quality observing frameworks, offering types of assistance going from sleep time checking to rest movement identification. Notwithstanding, as rest quality is firmly identified with the circulation of rest term over various rest stages, neither the sleep time nor the power of rest exercises can reflect rest quality definitely. We present Sleep Hunter, a portable help that gives a fine-grained location of rest stage change for rest quality checking and savvy reminder. The reasoning is that each rest stage is joined by explicit body developments and acoustic signs.

Utilizing the underlying sensors on cell phones, Sleep Hunter coordinates these proactive tasks with rest climate, inalienable fleeting connection and individual variables by a factual model for a fine-grained rest stage location. In light of the term of each rest stage, Sleep Hunter further gives rest quality report and shrewd call administration for clients. [4]. Xi Chen, Xiaopei Wu, Xiangyang Let al., has proposed in this paperaccurate maps are progressively significant with the development of PDAs and the advancement of area based administrations. A few publicly supporting based guide age conventions that depend on clients to give their follows have been proposed. Being inventive, in any case, those techniques represent a critical danger to client security as the follows can undoubtedly suggest client personal conduct standards. On the other side, publicly supporting based guide age strategy needs singular areas. To address the issue, we present a deliberate participatory-detecting based great guide age conspire, PMG that satisfies the security need of individual clients. To be explicit, the individual clients simply need to transfer chaotic inadequate area focuses to diminish the danger of uncovering clients' follows and use the Crust, a strategy from computational math for bend recreation, to gauge the unseen guide just as assess the level of security spillage. Investigations show that our answer can produce great guides for a genuine climate that is hearty to boisterous information. The contrast between the ground-truth map and the delivered map is under 10m, in any event, when the gathered areas are about 32m separated in the wake of grouping to eliminate commotion. [5]. Feng Wei, Wang Zhenget al., has proposed in this paper. These "directions for use" are planned to illuminate buyers about the right and safe approaches to utilize items, and they have a significant impact in securing buyers' very own wellbeing, their property and their own wellbeing just as in ensuring against natural contamination, forestalling misrepresentation and misdirecting data, and securing buyers' rights. .The present piece of GB 5296 is a significant drive and direction in creating different pieces of the public norm on "guidelines for utilization of results of customer interest", and encouraging the normalization of guidelines for use in China. The current part comprises of the overall standards of GB 5296, and as such it doesn't cover every one of the nitty gritty arrangements of guidelines for utilization of every classification of results of customer interest. Subsequently, the standards in the current part will fill in as broad arrangements for every one of the invested individuals in their plan and improvement of guidelines for use in every category.Information passed on to clients on the most proficient method to utilize items accurately and securely and on item works, fundamental properties, and attributes identifying with said items. [6]. Cheong Tak Leong, Robert Chewet al., has proposed in this paper. This determination depicts the specialized prerequisites for a shrewd card that can be utilized in a multiuser sending situation. Backers are answerable for the personalisation of their own cards. Interoperability is accomplished by different arrangements of keys dwelling in the terminal perusers and in the card. For interoperability, keen card perusers will contain charge keys of the multitude of partaking Issuers, however not their credit keys. Credit activity is subsequently restricted to chosen terminals (perusers) that contain the necessary credit keys. Key administration is intended to be adaptable and the last execution decision is left with the card Issuer. The charge order requires 1 key reference while the credit order requires 2 key references. In the least difficult case, every one of the 3 references (1 for charge, and 2 for credit) could all allude to a similar key. The plan permits incomplete discount, interestingly with a typical credit.

The incomplete discount is restricted to the latest sum charged. There is no limitation for a credit activity. [7]. Thomas Korak and Michael Hutteret al., has proposed in this paper A immense number of safety significant frameworks these days utilize contactless brilliant cards. Such frameworks, similar to instalment frameworks or access control frameworks, ordinarily utilize single-pass or common verification conventions to evidence the birthplace of the card holder. The use of hand-off assaults permits to bypass this confirmation cycle without expecting to assault the execution or convention itself. All things considered, the whole remote correspondence is just sent utilizing an intermediary and a mole permitting to transfer messages over a huge distance. In this paper, we present a few transfer assaults on an ISO/IEC 14443-based keen card carrying out an AES challenge-reaction convention. We feature the qualities and shortcomings of two diverse intermediary types: a NFC advanced cell and a devoted specially crafted intermediary gadget. To start with, we propose a "three-telephone in-the-center" assault that permits to transfer the correspondence over in excess of 360 feet (110 meters). Second, we present a uniquely crafted intermediary that addresses significant transfer assault limitations that apply on practically all NFC advanced mobile phones, for instance, cloning of the casualty's UID, adaption of low-level convention boundaries, direct solicitation for Waiting Time Extensions, or dynamic adjustments of the messages. [8].Michael Roland, Josef Langeret al., has proposed in this paper. The late development of Near Field Communication (NFC) empowered advanced cells brought about an expanding interest in NFC security. A few new assault situations, utilizing NFC gadgets either as assault stage or as gadget enduring an onslaught, have been found. One of them is the product based hand-off assault. In this paper we assess the attainability of the product based transfer assault in a current versatile contactless instalment framework. We give a top to bottom investigation of Google Wallet's Mastercard instalment usefulness. We depict our prototypical transfer framework that we used to effectively mount the product put together hand-off assault with respect to Google Wallet. We talk about the practicability and danger capability of the assault and give a few potential workarounds. At last, we break down Google's way to deal with settling the issue of programming based transfer assaults in their new arrivals of Google Wallet. [9]. Daniel J. Bernstein,NielsDuifet al.,has proposed in this papershows that a $390 mass-market quadcore 2.4GHz Intel Westmere (Xeon E5620) CPU can make 109000 marks each second and confirm 71000 marks each second on an elliptic bend at a 2128 security level. Public keys are 32 bytes, and marks are 64 bytes. These exhibition figures incorporate solid protections against programming side-channel assaults: there is no information stream from secret keys to cluster lists, and there is no information stream from secret keys to branch conditionsthe complete confirmation method takes under 134000 cycles for each mark for clump size 64. Our batch verification programming is remembered for, albeit not yet benchmarked by, the public e-BATS benchmarking structure. Multiplying the bunch size to 128 no longer finds a way into L1 reserve yet improves execution on our objective CPU, taking under 125000 cycles for every signature. [10].

8. Proposed Methodology

We make and evaluate a data disguising methodology that engages phones to scramble and embed tricky information into carrier surges of sensor data.

Our appraisal considers different handsets and a variety of data types, and we show that our methodology has a computational expense that grants steady data stowing away on PDAs with irrelevant curving of the carrier stream. These ascribes make it suitable for wireless applications including protection touchy data, for instance, clinical noticing structures and progressed legitimate sciences gadgets

9. Data Pre-Processing

In this module information pre-processing module serves to portray dataset handling performed on crude information to set it up for another preparing strategy. The primer information pre-processing changes the information into an arrangement that will be all the more effectively and viably prepared with the end goal of the client.

10. Tampering Entrance Data

We need to know two significant snippets of data: 1) the information construction of passage information, and 2) the station information, e.g., GPS scope and longitude facilitates. In this part, we depict an assortment of ways to deal with construe the above data

11. Obtaining Station Information

Instead of gathering station information by visiting each station (appears to be incomprehensible), we tracked down an outsider application called E-Card Tapper, which can parse the exchange narratives just as the outing records and subtleties. Driven by this discovering, we switched this application utilizing Apktool and unloaded the station information from the internal SQLite data set of E-Card Tapper to separate its put away station data, like the station identifier.

12. Tampering the Entrance Data

To alter the passage information. In the Less Pay execution, as, the web worker in the cloud is liable for producing the phony passageway information dependent on the above-gathered information. To misrepresent a piece of substantial passageway information, we essentially set up the real passage time, station data, and the equilibrium. To limit the passage, the aggressor's cloud needs to create the appropriate passageway information as indicated by the objective.

13. Relay Attack on AFC Card

It is difficult to imitate an AFC card with charge support. All in all, the test in this stage is the means by which we can get an exchange key TK for our copied card to make it pass the shared verification. We utilize the actual card outfitted with TK to sidestep this security check. At the end of the day, in Less Pay, the copied card ought to have a comparing actual AFC card in the cloud-side card pool.

14. Experimental Setup

We selected 100 volunteers to utilize Less Pay. These clients are outfitted with HCE Android advanced mobile phones. The telephone models we utilized are Samsung Galaxy S5, Huawei Mate 7, Moto XT1095, and LGE Nexus 5X. 62 clients use LTE-TDD organization, and the others use LTE-FDD organization. The investigation went on for a quarter of a year (from Jan. tenth to Apr. tenth, 2016). Every client was approached to utilize Less Pay 40 times each month, with an aggregate of 12,000 tests performed, regarding transmission capacity overhead, our deliberate outcomes show that the size of a solitary solicitation is 48 bytes (16-byte area and 32-byte client token). The size of a solitary reaction is 20 bytes (6-byte card number, 4-byte equilibrium, and 10-byte entrance information). Counting TCP handshakes, and TCP/HTTP headers, the complete organization traffic cost is under 1 KB. The total dissemination work (CDF) of organization traffic devoured in these 12,000 tests to comprehend the overhead of Less Pay on battery life, we record the battery power utilization in these tests. As demonstrated in Fig. 11, the normal force utilization per trip is 3.4 mWh, which is incredibly low given that the battery limit of well-known advanced cells lies between 5 - 20Wh.

15. Conclusion

The present AFC structures have been all around embraced and billions of AFC cards have been given wherever on the world. Among these structures, ISO/IEC 14443 is the principal show used around the globe, being near far and wide in East Asia and Europe, and in its underlying choice in the rest of the world. Under the above establishment, this paper proposes another exchange attack on AFC systems, which enables customers to pay altogether not exactly truly required by giving fake entry data. The exchange attack is adaptable and intangible to AFC system managers. We have developed a HCE application, named LessPay, considering our proposed and reported attack, and evaluated the LessPay application through genuine investigations. The evaluation results show the feasibility, sensibility and versatility of our strategy. To manage the fabricated hand-off attack, we finally propose four sorts of countermeasures against the created hand-off attack. We complete, pass on and evaluate these countermeasures, and besides give the assessment of these philosophies.

References

[1] "E-card tapper," http://www.wandoujia.com/applications/com.siodata.uplink, [Online; got to on July 20, 2016].
[2] C. J. Mitchell, "On the security of 2-key triple DES," IEEE Trans. Data Theory, vol. 62, no. 11, pp. 6260–6267, 2016.
[3] "MasterCard Contactless," http://www.mastercard.com/contactless/, [Online; got to on July 21, 2016].

[4] W. Gu, L. Shanguam, Z. Yang, and Y. Liu, "Rest tracker: Towards fine grained rest stage following cell phones," IEEE Transactions on Mobile Computing, vol. 15, no. 6, pp. 1514–1527, June 2016

[5] X. Chen, X. Wu, X. Y. Li, X. Ji, Y. He, and Y. Liu, "Security mindful high quality map age with participatory detecting," IEEE Transactions on Mobile Computing, vol. 15, no. 3, pp. 719–732, March 2016.

[6] "City association card of advanced city General innovation necessities," Standardization Administration of the People's Republic of China, Beijing, China, GB/T 31778-2015

[7] "Specification for Contactless ePurse Application (CEPAS)," Singapore Standards Council, Singapore, SS 518:2014.

[8] T. Korak and M. Hutter, "On the force of dynamic transfer assaults utilizing uniquely designed intermediaries," in Proceedings of the eighth IEEE International Conference on RFID (IEEE RFID), April 2014, pp. 126–133

[9] M. Roland, J. Langer, and J. Scharinger, "Applying transfer assaults to google wallet," in Proceedings of the fifth International Workshop on Near Field Communication (NFC), Feb 2013, pp. 1–6.

[10] D. J. Bernstein, N. Duif, T. Lange, P. Schwabe, and B.- Y. Yang, "Highspeed high-security marks," Journal of Cryptographic Engineering, vol. 2, no. 2, pp. 77–89, Sep 2012.

[11] Nandagopal S, Arunachalam VP, KarthikS, “A Novel Approach for Mining Inter-Transaction Itemsets”,European Scientific Journal,Vol.8,pp.14-22, 2012.

[12] V.S. Suresh kumar “Frequent Pattern Complex query management using FIUT Approach”, South Asian Journal of Engineering and Technology, pp: 300-304, issue 204, volume 202, 2018

[13] Gokulraj P and Kiruthikadevi K, “Revocation and security based ownership deduplication of convergent key creating in cloud”, International Journal of Innovative Research in Science, Engineering and technology. Vol. 3, Issue 10, ISSN: 2319-8753, October 2014.

[14] Sureshkumar V S, Chandrasekar A,” Fuzzy-GA Optimized Multi-Cloud Multi-Task Scheduler For Cloud Storage And Service Applications” International Journal of Scientific & Engineering Research, Vol.04, Issue.3,pp-1-7, 2013

[15] E.Prabhakar,V.S.Sureshkumar, Dr.S.Nandagopal, C.R.Dhivyaa, Mining Better Advertisement Tool for Government Schemes Using Machine learning “ , International Journal of Psychosocial Rehabilitation, Vol.23,Issue.4, pp. 1122-1135, 2019

[16] Prabhakar E, “ Enhanced adaboost algorithm with modified weighting scheme for imbalanced problems, The SIJ transaction on Computer science & its application,Vol.6,Issue.4, pp.22-26, 2018.

[17] Suresh kumar V S ,Thiruvankatasamy S, Sudhakar R, “Optimized Multicloud Multitask Scheduler For Cloud Storage And Service By Genetic Algorithm And Rank Selection Method”, Vol.3,Issue.2, pp.1-6, 2014

[18] Nandagopal S, Malathi T, “Enhanced Slicing Technique for Improving Accuracy in Crowd Sourcing Database”, International Journal of Innovative Research in Science, Engineering and Technology, Vol.3,Issue.1, pp.278-284, 2014

[19] Prabhakar E, Santhosh M, Hari Krishnan A, Kumar T, Sudhakar R,” Sentiment Analysis of US Airline Twitter Data using New Adaboost Approach” ,International Journal of Engineering Research & Technology (IJERT),Vol.7,Issue.1, pp.1-6, 2019

[20] V.S. Suresh kumar “E-Farming by means of E-Mandi Process”, International Journal of Research and Advanced Development (IJRAD), ISSN: 2581-4451, pp: 55-57, Issue 6, volume 2, 2019

[21] S Nandagopal, S Karthik, VP Arunachalam,” Mining of meteorological data using modified apriori algorithm”, European Journal of Scientific Research , Vol. 47, no.2, pp. 295-308, 2010.

[22] P Gokulraj, K Kiruthika-Devi,” Revocation and security based ownership deduplication of convergent key creating in cloud”, International Journal of Innovative Research in Science, Engineering and Technology, Vol. 3, no.10, pp16527-16533, October 2014.

[23] E Prabhakar, R Parkavi, N Sandhiya, M Ambika,” Public Opinion Mining for Government Scheme Advertisement”, International Journal of Information Research and Review, Vol. 3, no.4, pp2112-2114, February 2016.

[24] E Prabhakar, G Pavithra, R Sangeetha, G Revathy,” MINING BETTER ADVERTISEMENT TOOL FOR GOVERNMENT SCHEMES”, International Journal For Technological Research In Engineering, Vol. 3, no.5, pp1023-1026, January 2016.

[25] Karthik.S. Nandagopal.S, Arunachalam.V.P.,” Mining of Datasets with Enhanced Apriori Algorithm”, Journal of Computer Science, Vol. 8, no.4, pp599-605, 2012.

[26] E. Prabhakar,” ENHANCED ADABOOST ALGORITHM WITH MODIFIED WEIGHTING SCHEME FOR IMBALANCED PROBLEMS”, The SIJ Transactions on Computer Science Engineering & its Applications (CSEA) , Vol. 6, no.4, pp22-26,July 2017.

[27] Nandagopal.S. Malathi.T.,” Enhanced Slicing Technique for Improving Accuracy in Crowd Sourcing Database”, International Journal of Innovative Research in Science, Engineering and Technology) , Vol. 3, no.1, pp278-284,2014

[28] V Dharani S Thiruvenkatasamy, P Akhila, V Arjitha, K Bhavadharani,” A MD5 Algorithm Approach to Monitor Village Using Mobile Application”, South Asian Journal of Engineering and Technology, Vol. 8, no.s1, 2019.