International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 03 | Mar -2017 www.irjet.net p-ISSN: 2395-0072

Demonetization in Indian Currency – Illegal Money - IOT: EFFECTIVE IDENTIFICATION OF BLACK MONEY, FAKE CURRENCY & EXPIRY USING NFC, Internet Of Things & ANDROID

N.Lalieth Kumar[1] T.Reddy Hemanth[2]
[1]. 211413205302 [2]. 211413205083
Student
Department of Information Technology
Panimalar Engineering College
Mr.Balasundaram
Associate Professor
Department of Information Technology
Panimalar Engineering College

Abstract **–**The main aim of our project is to eradicate black money and effective removal of fake currency in the trade market to make this effective we have came up with the new concept of embedding NFC chips in to our currency notes making it traceable and reusable this tag includes the rupee value, tag number and expiry date of currency. We are implementing 4 methodologies for identifying the black money. In every office/shops we are going to provide money counting devices which comes with a inbuilt RFID reader which would read the currencies tag no, value and expiry date. We would provide a RFID reader device which can be attached to the android mobile via OTG connectivity to all the small entrepreneurs and road side vendors. For merchants and vendors who cannot afford a reader we generate QR codes with respective details of the person's account So the buyer can scan the QR code which contains the account details of the Person and pay the amount will be credited to the sellers account. We are implementing cashless transaction using card. Using all of the above four methodologies RBI can easily track all the transactions (Income & Expenditure) made by every individual user. One more feature is we provide SMS notification for expiring currency.

Keywords- NFC : Near Field Communication, RFID : Radio Frequency Identification, QR : Quick Response, OTG : On The Go

I. Introduction:

HF-based RFID and NFC systems are widely spread nowadays. They can be found in our everyday lives, in applications such as payment, transportation and logistics, healthcare, and access control systems. A particular boost has been recognized since RFID/NFC reader functionality has been integrated into a vast amount of smart phones. The basic principle of such a contactless RFID/NFC system is illustrated. The reader device emits an alternating magnetic field, which is used to power the transponder and to exchange data with it by means of modulation. The achievable reading distance of such a contactless and passive system depends on several factors. One of the most important factors is the size of the antenna: the larger the antenna, the better the coupling. However, the smaller the antenna and the tags are, the higher is typically the variety of products that can be tagged. If such transponders are manufactured small enough, then they can be integrated into various products, casings, or consumable materials in a discreet way. Since counterfeiting of designer products is reported as a major issue with a global economic value of over $ 865bn, as one can see in Table I and in [2], a simple, small-sized, and secured way to check genuineness is eligible. Given this motivation, it is of highest interest to provide small-sized and secured RFID technology, which can be integrated into products in a very discreet way and which can be verified in terms of authenticity with commonly available RFID reader devices. However, to the best of our knowledge, there is a major gap in industry and in academia concerning this field of application. This work addresses the outlined gap and presents a miniaturized, system-in-package, contactless and passive authentication solution that features NFC and state-of-the-art security measures. This is achieved by integrating Infineon Technologies'

CIPURSET Move chip, which is a security chip featuring an open security standard, into embedded Wafer Level Ball Grid Array (eWLB) packages, together with HF-antennas, ferrites, as well as discrete elements that improve HF-coupling characteristics. Thus, a system-in-package security solution is given that enables not only the anti-counterfeiting use-case, but also micropayment, ticketing, access control, and password storage. Summarizing, this paper makes the following contributions: It introduces the novel system-in-package contactless Authentication devices. It details design and implementation decisions as well as simulation results. It proves the applicability of the fabricated devices by means of an access control demonstrator. This paper is structured as follows gives a short introduction into the related work covering the topic of small-sized RFID solutions.

II. Assistive technology

Radio-frequency identification (*RFID*) uses electromagnetic fields to automatically identify and track tags attached to objects. The tags contain electronically stored information. Passive tags collect energy from a nearby RFID reader's interrogating radio waves. Active tags have a local power source such as a battery and may operate at hundreds of meters from the RFID reader. Unlike a barcode, the tag need not be within the line of sight of the reader, so it may be embedded in the tracked object. RFID is one method for Automatic Identification and Data Capture (AIDC).

RFID tags are used in many industries, for example, an RFID tag attached to an automobile during production can be used to track its progress through the assembly line; RFID-tagged pharmaceuticals can be tracked through warehouses; and implanting RFID microchips in livestock and pets allows positive identification of animals.

NFC is a set of short-range wireless technologies, typically requiring a separation of 10 cm or less. NFC operates at 13.56 MHz on ISO/IEC 18000-3 air interface and at rates ranging from 106 kbit/s to 424 kbit/s. NFC always involves an initiator and a target; the initiator actively generates an RF field that can power a passive target. This enables NFC targets to take very simple form factors such as unpowered tags, stickers, key fobs, or cards. NFC peer-to-peer communication is possible, provided both devices are powered.[34]

NFC tags contain data and are typically read-only, but may be writeable. They can be custom-encoded by their manufacturers or use NFC Forum specifications. The tags can securely store personal data such as debit and credit card information, loyalty program data, PINs and networking contacts, among other information. The NFC Forum defines four types of tags that provide different communication speeds and capabilities in terms of configurability, memory, security, data retention and write endurance. Tags currently offer between 96 and 4,096 bytes of memory.

III. Scope

The scope of this project is integration of RFID, IOT and Big Data. Multi User, Multi Account chip embedded rupee note is implemented. The user behavior is tracked using Formulae Authentication is implemented for Security. Easy and comfortabl Transaction with security. Multiple user bank accounts can be identified by the RBI and black money fake currency can be completely eradicated using these methods.

IV. Existing systems

V.

The market size of NFC-based payment services is expected to be increased to $3.572 and $180 billion in the years 2015 and 2017 separately . Since the rapid development of short-range wireless communication technology, there is a growing demand to design secure and efficient mobile applications, such as service discovery, epayment, ticketing, and mobile healthcare systems, etc., in the area of the consumer electronics for NFC. In the NFC environment, the Trusted Service Manager (TSM) is responsible to distribute user keys to the registered users based upon the requests from the users and it does not involve in the authentication process. The authentication protocol involves only two parties, namely, an initiator user and a target user. The initiator user generates a radio frequency field and starts the NFC interface. After receiving communication signals, the target user sends a response message to the initiator user through the radio frequency field. After mutual authentication, both the initiator user and target user establish and agree on a secure session key. Due to the shared nature of wireless communication networks, there are several kinds of security vulnerabilities in NFC environment including impersonation and man-in-the-middle attacks. Thus, the security is one of the prerequisite for NFC applications . Moreover, transmission capacity of NFC technology is limited as its operating frequency is 13.56 MHz with transmission speed ranging from 106 Kbps to 424 Kbps up to 10 cm .

Since the widely use of mobile devices, such as smart phones and personal laptops, in combination of NFC technology, authentication protocol must ensure high security along with low computation and communication costs

VI. Principle of operation

we first investigate the classic tax evasion cases, and employ a graph-based method to characterize their property that describes two suspicious relationship trails with a same antecedent node behind an Interest Affiliated Transaction (IAT). Between the transaction parties the most important thing is that there exists a complex and covert interactive relationship. For example, if there exist. In our implementation. RFID tag is attached with the rupees note, in this tag includes the rupee value, tag number and expiry date of currency. We are implementing 4 methodologies for identifying the black money. 1. In every office/shops we install money counting device which would read the currency like tag no, value and expiry date. 2. We would provide reader device which can be attached to the mobile via OTG connectivity to any of the merchants/vendors. 3. QR code - In case of small vendors like street business merchants (vegetable selling people). So public can scan the QR code which contains the account details of the server. Automatically amount would be credited to the sellers account. 4. We are implementing cashless transaction using card. Using all of the above four methodologies RBI can easily track of all the transactions (Income & Expenditure) made by every individual user. One more implementation is SMS notification for expiry currency.

VII. Architecture diagram

Figure.1. Architecture diagram of Demonitization

VIII. Advantages

All the transactions are accounted Can be track completely Latest technology like QR code is implemented Also this system motivates cashless transaction This system will totally eradicate black money SMS notification for expiry currency

IX. Conclusion

In this project we are implementing four methodologies. Using 4 methodologies RBI easily can track of all the transactions like income and expenditure made by every individuals users/merchants or vendors. This is directly compared with the total audit report provided by this by these people. This system will strongly eradicate the black money process. Also in case expiry the currency means automatically notification to user.

REFRENCES

[1] D. S. Almeling, "Seven Reasons Why Trade Secrets are Increasingly Important,"*Berkeley Technology Law Journal*, vol. 27, no. 2, pp. 1092–1118, 2012.

[2] L. Antunes, J. Balsa, and H. Coelho,"Agents that Collude to Evade Taxes,"in*Proc. 6th Int. Conf.Autonomous Agents and Multiagent Systems (AAMAS)*, pp.1263–1265, May.2007.

[3] Y.S. Chen and C.-H. Cheng,"A Delphi-Based Rough Sets Fusion Model for Extracting Payment Rules of Vehicle License Tax in the Government Sector,"*Expert Systems with Applications*, vol. 37, no. 3, pp. 2161–2174,Mar.2010.

[4] M. J. Ferrantino, X. Liu, and Z. Wang,"Evasion Behaviors of Exporters and Importers: Evidence from the U.S.-China Trade Data Discrepancy,"*Journal of International Economics*,vol. 86, no. 1, pp. 141–157,Jan.2012.

[5] W. F. Fox, L. Lunab, and G. Schau,"Destination Taxation and Evasion: Evidence from U.S. Inter-State Commodity Flows,"*Journal of Accounting and Economics*,vol.57, no. 1, pp. 43–57, Feb. 2014.

[6] Z. Gao,"Transfer Price-Based Money Laundering: A Transit Trader'sPerspective,"in*Proc.4th Int.Conf.Wireless Communications, Networking and Mobile Computing(WiCOM)*, pp.1–5, Oct.2008.

[7] P. C. Gonz´l´cleza and J. D. Vel´l´csquez,"Characterization and Detection of Taxpayers with False Invoices Using Data Mining

Techniques,"*Expert Systems with Applications*,vol.40, no. 5, pp. 1427–1436, Apr.2013.

[8] N. Goumagias, D. Hristu-Varsakelis, andA. Saraidaris,"A Decision Support Model for Tax Revenue Collection in Greece,"*Decision Support Systems*,vol.53, no. 1, pp. 76–96, Apr.2012.

[9] J. Han, M. Kamber, and J. Pei,*Data Mining: Concepts and Techniques*,Burlington,Massachusetts: Morgan Kaufmann,2011.

[10] J. Hasseldinea and G. Morris,"Corporate Social Responsibility and Tax Avoidance: A Comment and Reflection,"*Accounting Forum*,vol.37, no. 1, pp. 1–14, Mar.2013.

[11] L. Kaplow, A. Polinsky, and S. Shavell,*Handbook of Law and Economics*, vol.1, chap.10, Elsevier Science Ltd,pp.647–755,Aug.2007.

[12] Y. Kim, Savoldi, H. Lee, S. Yun, S. Lee, and J. Lim,"Design and Implementation of a Tool to Detect Accounting Frauds,"in *Proc.Int. Conf. Intelligent Information Hiding and Multimedia Signal Processing(IIHMSP)*, pp.547–552, Aug.2008.

[13] X. Liu, D. Pan, and S. Chen,"Application of Hierarchical Clustering in Tax Inspection Case-Selecting,"in *Proc. Int. Conf.Computational Intelligence and Software Engineering (CISE)*, pp.1–4,Dec.2010.