International Journal of Computer Architecture and Mobility
(ISSN 2319-9229) Volume 3 -Issue 2, April 2015

Augment The Use Of Plastic Money And Virtual Wallet Services By Emphasizing the Need to Reduce Digital Footprints

Surya Pratim Kesh[#1], Dr. Mousumi Majumdar[#2], Dr. Sukanta Chandra Swain[#3]

Surya Pratim Kesh ICFAI, Research Scholar, University Jharkhand, Ranchi
Dr. Mousumi Majumdar Research Supervisor, Vanguard Business School, Bangaluru
Dr. Sukanta Chandra Swain, Research Guide, Asst. Dean, ICFAI University Jharkhand, Ranchi

Surya.kesh@gmail.com
Mousumimajumdar@gmail.com
Sukanta@ibsindia.org

***Abstract*— Digital Anonymity is desired to the extent of protecting your Personally Identifiable Information. Malwares, social engineering attacks and many others are making our life difficult and threatening the banking sector. "Dyre Wolf Malware" is one of the latest attacks that have been detected and there would be many unreported once. It is estimated that this single malware may have stolen already stolen over $1 million from large and mid-sized companies. This coupled with the fact that most users have common and easy to guess password and the secret question for retrieving banking password is easy to retrieve by social engineering. Digital footprints are generated by you and everyone you know in the virtual or digital space. Research has established that 33% [1] of your profile is searched by your colleges and it is easy to get your information from your colleges and your professional /personal networks. This paper explores the simple methods of using credit cards and debit cards to protect yourself and others along with the new business models.**

***Keywords*— Credit card, debit card, mobile wallet, USSD, virtual money, bitcoin, digital footprints**

I. INTRODUCTION

Current age of information technology is making rapid progress in the field of payments and there are numerous business models built around the new payment scenarios.

The amount of digital footprints per individual is difficult to ascertain and it is growing as we collect every possible data for the individual. Data collected by various sites can be compromised and used for social engineered attacks. In this light it is paramount important to understand how companies and individuals secure themselves against attacks in the current situation.

Digital footprints are left by users, friends and online community. It is augmented by big data mining techniques and machine learning over the years to create an users digital profile. This coupled with the fact that emails are almost never deleted, chats are achieved and voice over internet can be easily analyzed makes it a difficult for anyone to hide ones identity.

Bitcoins and equivalent methods of anonymous payments are in its infancy and does not always offer anonymous payment solutions.

An attempt has been made in this paper to evaluate the impact and promote the use of debit and credit cards for enhanced security. This paper attempts to promote the debit and credit card as an entity that is available in multiple forms like plastic, chips, mobile wallet etc. the physical form of this card can be plastic or this can be a virtual entity.

We also cover this from the Indian perspective where the India's illiterate population is the largest in the world as per UNESCO report. Apparently India is working towards financial inclusion which would mean an increase in debit and credit card for the poor and uneducated masses. It is important to protect the investment of the masses to gain the confidence of the payment system. The national pay commission has been introducing new clearance process which is fast and also does auto settlement/clearance. In light of this latest development, it would be difficult to control the small payments scenarios if we do not use the digital payments judiciously.

[1]Source (milfordpublicschools.org) _https://sites.google.com/a/milfordpublicschools.org/digital- footprint-and-reputation/facts

[2] India's illiterate population is the largest in the world as per UNESCO report. Source (the hindu.com) http://www.thehindu.com/news/national/indias-illiterate-population-largest-in-the-world-says-unesco-report/article5631797.ece

The Indian society is different from many others as the laptop or mobile is generally used by the family rather than a single individual. There are the cyber café where the system is shared with the unknown users who cannot be traced. In these scenarios, it becomes difficult to control the system and it would be difficult to hold a single individual responsible for all the activity done on a machine or mobile device. This paper looks at using or augmenting the existing features of the cards to make a digital transaction secure.

II. Understanding Digital Footprints

Digital FootPrints are traces of digital information a user leaves while surfing the internet/web. Any user who uses the web leaves a trace which can potentially be used to identify and track the user information. This is more prominent with users using social media sites and creating profiles in different websites, e-commerce and m-commerce space.

With the advance and the recent advances in technology it is easier to collate information and track the users over a long period of time. This can be achieved using an assortment of technology from analytics, big data, and machine learning to social engineering hacks.

Coupled with the fact that we are living in a highly networked environment, it is easy to collect the information from personal, private and social networks.

A more challenging development in this space is the data explosion with the advent of Internet of things and the cloud. Data is stored in virtual space which is accessible to government and other agency.

A. User Leaving Personal Digital Footprints

Every user using the web has registered to some website or another and most of the users have multiple profiles. Some people have fake profiles as well as a professional profile like some job sites and other places. Few of these social sites allow controlled access to user data based on users profile setting and most of the sites have introduced telephone number as a two factor identification method for greater security which can be made available to third parties based on policy settings.

Let us describe the threat with an example. The article from the website on Digital Footprints weebly.com "digitalfootprintimu.weebly.com" states that 87% of Americans can be identified online with just three facts about them: ZIP code, birthday, and gender. It is not difficult to collect the zip code which is probably the recent of most frequent location or sometimes same as the ZIP of the shipping address given in any e-commerce site. Birthday and Gender Data is mostly available in social sites but sometimes it has to be collected via some online birthday calendar, email and from the chat logs in various sites.

B. Personal or Professional Network leaves Digital Foot Prints

With the manifold increase in data and the linkage between the user and other members of his professional, social and personal network can increase your digital footprint many more times than expected. The digital data from individual can be collated to generate actionable data set. It is also an important element of social engineering hacks which can aim at getting sensitive information from simple things like family photos, group photos and email forwards. Once you data is available in the internet it gets replicated in various forms which increases your digital footprint and the data cannot be erased easily.

Many people have fake profile or put fake information in their existing profile which can also be detected by seasoned attackers.

It is estimated that most of the users visiting your public profile are friends and colleagues which can be used to weed out and gather your workplace information and social linkages.

C. Special Usage Scenarios That Increase Your Digital Footprints

There are various scenarios which increases your digital footprints like use of cyber café in India. In India where many people still visit cyber Café to access internet, exposes them to many threats. Sometime they leave documents on the desktop and many times the history is not erased. These places wherein community or family members collectively use a device are risking their identity even when the user is very cautious not to leave the digital footprints.

In India the IP address or location tracking can hacker's valuable clue to reach the Cyber Café Owner. Once the Cyber Café is identified the telephone numbers of the Café is available on the internet which can be used to track the individual.

Tagging is another form of linking your text data to pictures and the picture search can provide additional information about every user.

D. Malicious Code, Malwares and SSL Hacks

Malwares can create hooks to collect information from your browser and cookie. Some malwares can take your picture without any warning or approval. The malwares can collect useful data by taking screenshot's as well. This data augmented with data compromised when big corporations are hacked or when SSL hacks like Heartbleed etc. can break security barriers.

E. Hypervisor and OS Security controls

Till recently many kinds of security was concentrated on physical security of the box, authentication and authorization and few other security measures. Hypervisor security has recently been increased to protect virtual and physical boxes. This is also an important security entry point which if compromised can give away the files and other information stored in your personal box. In India the threat is even more as most of the computers and devices are used by multiple people and some of these do not apply security patches regularly.

F. Telephone Records and New sources of Information

With the advent of telephone, it is easy to tap and analyze the digital data sent over the wires as the latest digital technology makes it easy to collect valuable information like location and user information. Data collected over a period of time can help in understanding the person and his network. It can also give way to the daily routine of the user and once the data is collected over years, it is ready to be used in machine learning.

Machine learning is not new but over the years the machines have learnt how to trace patterns and make deductions. All this can help in identifying people information and collate this data with the digital footprints of the user.

A combination of all this data makes a person susceptible to attackers.

G. IOT and Augmented Digital FootPrints

Internet of things is a collection of sensors which convey the sensory data over the internet for other applications or user consumption.

A new threat is lurking around the horizon. Once we are trying to build like IOT which is Internet of things. IOT would be the most valuable source of information on the planet going forward as user data can be collected without the user's knowledge and even when the user is not online or carrying any mobile device.

With the influx of the IOT technology the user would be more and more susceptible and can be tracked without any physical or virtual intervention. This would make the non tech users as potential victims. A collection of tangled data set and social

information collected via friends and family using the internet can reveal the identity of any offline user.

H. Smart city, Smart grid, Cloud Technology, data Storage a boom for Digital Footprints based attacks

Smart city, cloud and other storage technology is a great blessing provided it is used safely but with the proliferation of applications, roles and data expansion, it would be impossible to ensure data security. What makes it even difficult is the fact that the data is available to a larger community and audience who may lose this data because of negligence or due to sinister motive.

Some email providers store all the emails you have ever sent and would be able to create your family tree, friend's tree and social interaction patterns. All this and much more would increase your digital footprint without your knowledge.

I. The use of Grids Computing for Collecting Digital Footprints and Brute force Attacks

While many think that the era of grid computing is fading as more powerful computers are available and it is not necessary to have a collection of devices to process a task, it is not really true. There are many payment systems like BITCOINS which may use grids and similar technology to process vast amount of information and collate it with a user. Once the data is revealed in such anonymous payment scenarios, it may not be possible to remain anonymous over the anonymous network. Once a transaction is tagged to an individual, the same can reasoning can be applied to track subsequent payments from the device.

While the payment industry is trying to create anonymous payment systems, a simple thing like logging in to another site from the same browser can reveal the identity of the anonymous payee.

J. Indexing Engines can give away your personal information

Yet another payment threat is the Indexing engines. There are many indexes which are indexing people, their names and other information. These sites have made it easier to weed out the spurious and fake social profiles from the useful once. Once the data is cleansed, the hackers can use the digital footprints better than ever before.

III. HOW DIGITAL FOOTPRINTS ARE MISUSED

From the previous section you would have understood that the amount of digital data collected and processed can lead to you. This can be a serious threat to payment security as most of the payment security standards are not geared to tackle all the challenges.

Payment technology is itself evolving at a rapid pace and making inroads in many new forms. Ranging for anonymous payments to Oauth based payments; the industry is evolving at a rapid pace. Some of the emerging standards are still at its infancy.

The recent example would be "Dyre Wolf Malware" which sits passively on an infected system and collects all contact data and hooks onto the browsers. The system remains dormant till a banking site is accessed. The malware activates and collects as much information as possible for every banking site visited. This coupled with the social engineering hack to collect the user information can help in carrying out online payment and withdraw large amounts of money.

Given below is a brief introduction to few technologies that can be misused to collect your information.

A. Machine Learning and Big Data Mining To Produce Reliable Digital FootPrints

Machine learning can be used to track regular patterns from a big set of random data and events. The machine learning is superior to do repeated task and there is potential to use this for collecting dataset collected over social, IOT, phone, VOIP, media, emails and if the current process gives better view of the digital footprints and machine learning can collate the information over a period of time and repeat the malicious activity time and again for many payment scenarios.

This leads to rapid analysis of the data set and is quickly executed before others can detect the loophole.

B. Omnichannel Payments and Security Risk

The omnichannel data is used for quick and easy payments in many scenarios and the same user profile information can be used across to close a deal and the money transfer. Many channels have shifted from using secure gateways and are using wallets and other methods for payments. Although these methods are evolving and does not have adequate security across the channels the way it is done in Banking Gateways, Visa and Master cards. The one click payment uses a variety of mechanism and profile information to reduce the risk of money transfer but is not full proof. As the apps boom, some of these apps do not strictly regulate the session and payment timeout which can be misused. As little or no information is collected during payment, it is difficult to ascertain any frauds quickly across the channels. Some of the apps do not enforce single login across different channels as a result of which the Omni Channel payments can be initiated by multiple devices.

There are hacks wherein the information is relayed multiple times and the intercepted data is not manipulated. The Digital footprints give sufficient information on the geolocation of the user and the home location of the user. Such Digital information can be used by the hackers to replay or execute attack from machines located in similar geography thus bypassing any fraud detection algorithm checking geolocation.

C. Analytics Can Help Hackers Find Soft Target

Analytics has made tremendous advancement but the same method can easily point out soft targets via digital fingerprinting.

Analytics can sample out data set of user showing a large volume and value payments. As these users carry out frequent transactions, slight negligence or mistake can give out sensitive information. Such users also tend to have large digital footprints as they buy products frequently from multiple sites and tend to keep similar password and secret question. Frequent users also take decision after looking at peers and similar user groups which can further spread the attack.

IV. REDUCING YOUR DIGITAL FOOTPRINTS

While it is important to reduce the digital footprints, it is also important to protect personal information. Every picture or update need not be published in the internet and every person in your circle need not know all about you. While younger generation is fast and tech savvy, it is this group that has the largest digital footprint information that can be used against them. Payments done by students are generally of lower value but once they join workforce, the personal identifiable information can be used for the entire life of an individual giving a long term risk. In light of this it is important to teach every people to reduce and control their digital space. Special emphasis should be given to younger generations who is getting used to the online world.

A. Transactions In Banking Industry And Leaving Digital FootPrints

Special care must be taken while using banking channels. Pissing is common and some banks have introduced photo based identification to ward of attackers. It is important to avoid using public cyber café for payments. Transactions in the banking industry typically rely on the pin identification which is increased from 4 to 6 digits in some cases. In most of the mobile and e-commerce site there are options to use credit and debit cards and secure payment gateways, it would be worth to use these channels as banking channels are secure and does not leave enormous digital footprints the way it is done by wallet technology. Most of the banking gateways notify the website once the transactions succeed or fails but do not pass any unwanted information to the website, thus reducing the digital footprints.

There are different kinds of risks from malwares and spywares which can sniff and send users banking credentials to third parties. While keeping

updated security essentials can reduce the risk, the risk is not entirely mitigated. It is important to minimize the risk by using the virtual keyboard, picture security, CCV and other secret information to reduce this risk.

Another way to reduce the digital footprint is to make most of your purchase from few credible websites and not providing any personal data to these sites. Most of these sites do not require your exact name nor date of birth, etc which means you need not give accurate information out to non reliable websites. These websites only care about the payment done via banks or other channels and do not need all of your personal identifiable information. In fact it is better to leave the site which requires sensitive personal information for a payment transaction. Remember that even banking gateways do not ask for your personal information except probably your card no, name or login information and so the website also does not need all accurate data as of today.

B. Proposed Security in Omnichannel and Social Channel Using Cards

Extending the case mentioned above a little further to omnichannel, it is important to opt for two phase security mechanism and these should use two different devices. The concept of one time password assumes that the password would be sent on a secure device. This security is breached when users use the same smartphone to initiate a payment and also receive SMS. There are SMS readers and sniffer application can pose a serious challenge to the one time Password protection. New powerful malwares would even read your SMS and send the One Time Password to the hacker thus rendering the OTP security useless.

There are security software's that encrypt all your passwords and card numbers to provide greater online security in Mobile wallets and other mobile payment mechanisms. Users should opt for visa , MasterCard , rupay and similar cards or google wallet and apple pay only as of today. Visa and master cards have been around for more than thirty years in India and more elsewhere. These companies have sophisticated algorithms to detect frauds and have learnt to handle transactions over the years. Paypal is making great progress due to the increase in online payments and is considered reliable and secure. These are large organizations that can assure that your data is not shared to third parties and reduce your digital footprints. Credit and Debit cards are secure as the users address is verified in person and can the user is known to the banker only. Intermediary in the omnichannel using new payment mechanism tend to give out lot of public information or collect similar data repeatedly thus increasing the digital footprint.

Mobile point of sales or mPOS is a specialized system that deals with sophisticated payments. Banks should advice the use of mPOS system which can have card readers and various other advanced security features. There is less chance of a non card holder executing a payment transaction as the hacker does not have your physical card.

The systems like mPOS are also evolving and would be a better mechanism which banks should encourage. Most users would vouch that security is more importance than convenience and the latest mPOS systems are sleek and portable. Each mPOS system can easily read your card data and utilize the secure payment gateways thus effectively reducing your digital footprints.

C. Additional Security for Mobile Wallet Enhanced Security Using Picture Based Identification

Cleaning unwanted apps and cache should be done on mobile phones. There are security applications that warn you each time the mobile sends data automatically.

i. End to End encryption

Mobile payments in mPOS and card readers are using end to end encryption and routed via secure channels thus making ensuring end to end data security. While many emerging payment methods try to adhere to the security standards, it does not

take much to guess that they would need time to set right the end to end scenarios.

ii. EMV and PCI compliance

EMV have set up innovative payment systems that can address most of users need once they are part of the credit card or debit card network. Some of the convenience features are not used by banks and most of the masses are not aware of the features. Banks should aggressively promote these advance and convenient security features [3].

a) Card not present transactions over telephone or internet

b) Dynamic passcode authentication technique

c) Chip based authentication for e-commerce by MasterCard.

PCI [4] compliance for cards ensures that the companies and intermediaries that process credit card information do so in a controlled and standard manner. Banks should educate the customer to use the existing secure network as the new payment vehicles have not evolved standards to control end to end transaction scenarios.

[3] Source (wiki) _http://en.wikipedia.org/wiki/EMV

[4] Source of PCI compliance https://www.pcicomplianceguide.org/pci-faqs-2/#3

iii. Proposed Image Based Identification and secret keys for Security and Forgot Password Option

In India banks like HDFC uses picture based identification technique and ICICI has a sequence of pre-printed numbers and the corresponding secret on the card itself. This is seen as an set of CVV number rather than just once. The system challenges the user to key in a sequence of correct numbers by matching the same from the card itself. This would make it difficult for people to use the card until they have the card at hand. This feature has a problem as credit cards can be photocopied and the user loses the security cover. A combination of image and secret keys can make the card payment more secure while adding minimal overhead.

Bankers should promote the use of these add on features. These card features along with the terminal security and terminal verification enforced by EMV can help in validating the transaction.

UDDI based transactions lack this layer of security and are vulnerable to few of the prominent attacks. One of the prominent attacks is when a payment transaction is auto initiated or initiated via socially engineered hacks. Many uneducated users or first time users feel they are using an application but this may result in firing a UDDI based payment.

D. Controlling Digital Presence in Social Channels and Social Profiles

While it is important to build the professional and personal network for each individual, it is important to ensure that each digital channel does not give out personal identifiable information when users leave their digital footprints which can be used during payments. The issue with this approach is that the digital footprints are left by users and the people in their network.

Some of the methods like deleting old emails, not sending personal information over the network, deleting old post and searching the web regularly for your name can help you estimate the digital footprints you have left in the online world. This would help you control certain aspects of your online behavior and the behavior of your friends and other people in your network.

V. ALTERNATE METHODS OF VERIFICATION

Users should be encouraged and educated to use websites and payment gateways that strictly follow Two Factor Authentication, One Time Password and other security measures. Some of the gateways also track and aggregate the activity from particular websites and rank them based on the number of fraudulent cases detected or reported. It is my personal opinion that websites must be ranked by the security level and the number of frauds detected or reported. Alternate verification method should be activated is the payment is considered unsafe. This would be a different from the current fraud

detection on individual activity and a websites security rank can give an early warning to the payment systems.

VI. THE RIGHT TO BE FORGOTTEN CAN GIVE BETTER SECURITY TO USERS

Currently the users do have an option to prevent cookies and sites from collecting non personal data sets and customize the advertisement for each user. There are strict legal rules in few countries that mandate or bar the collection of user information.

VII. CONVENIENCE VERSES SECURITY

It is evident that the payment industry needs to build more security layers than ever before and most of the users when educated would see the advantage of using cards over complete digital payment system. As of today Convenience is the driving factor for much payment innovation but for users security and reasonable convenience would definitely be the first priority. It is a struggle to maintain the right form of digital identity and there are little known ways to standardize the digital identity of users. Credit cards and debit cards hardly reveal any personal identity of the user and should be considered the most optimal way to handle payments as of today.

VIII. HOW BANKS CAN DRIVE SECURITY AND LOW DIGITAL FOOTPRINTS

The role of banks has increased in the new age where banks should advocate and educate users to use the best technology and the safest method for online payments. None of the new payment modules would ever declare themselves as unsafe or even risky. So it is for the banks to educate the customer to protect the interest of the user and society. A wrong transaction or even news of fraudulent transactions sends ripples across the world and decreases user's confidence in the payment systems and instruments.

In this lie it is a series of action has to be taken by banks right form customer education to different risk management strategy for various devices, channels, apps and geography. As such the total responsibility of the banks would

A. By Promoting Cards

Banks have to promote the use of cards in physical and virtual forms like the once stored in google wallet to use the existing secure payment infrastructure and avoid many unknown pitfalls in the new and upcoming payment methods.

Ad campaigns targeting the users should emphasize the need and importance of security compliance measures like PCI and EMV. Customer awareness advertisement should also talk about the end to end payment security and fraud detection.

A prominent feature in some cards is the guarantee that liability for each fraud is born by the company and the users gets the money back. Banks should advocate the use of chip based security should help customers understand that chip based payments are one of the most reliable methods available today.

B. Old Is Gold: Payment Gateways Can Be Used For Secure Transaction

Online payments for various e-commerce and m-commerce scenarios should still promote the use of payment gateways by reducing the transaction charge or giving additional security features. These gateways should ensure that the least digital footprint is generated and most of the information in cookies and browsers is removed after the transactions. The masses should also be educated that there are session based hacks which and many other forms of hacks which may not be handled adequately by the new payment methods.

IX. DIGITAL FOOT PRINT REDUCTION FOR INDIAN MASSES

As discussed earlier India has large number of uneducated masses which have been bought under the payment system by the new government schemes which promote direct payment of subsidy to user's bank accounts and insurance cover.

A few measures have been suggested for the Indian scenario which may as well be considered

for other purpose. Physical security of ATM, cards and POS in India is a separate consideration and we focus on few other aspects here.

A. *Many Indians who are new to the use of cards and do not have sufficient education and are at risk.*

For Indians who are new to cards and similar banking instruments, it is better to use a combination of picture based and pin based security. The six digit pin from RuPay is long enough to ensure better security and is not too long to compel the user to write it on a piece of paper.

Customer awareness videos should be displayed in local languages at point of sales, ATM and other location educating the customers the importance of securing PIN.

B. *Mobile Currency and Mobile Payment Models are better for Countries like India*

The recent advances in mobile money transfers are better suited for countries like India as there are designated mobile stores where the money can be withdrawn. These stores are run by trained and get familiar with the mobile payment methods quickly after executing large sets of transactions.

For the customers this is convenience as they can go to the nearest store and also get professional help from these stores for the mobile based transaction.

This also minimizes the use of personal identifiable information over the wire and is considerably safe for use. It is evident that this mode of money transfer would gain popularity quickly as there is always a nearby store that can help them when required.

C. *Proposed Delayed Transaction and Confirmation*

Some non-conventional ways to increase security in each payment process would be to introduce a delay in actual payment by holding the balance in an escrow account.

This would be useful as there are many uneducated users who would be asking their friends and relatives to help them use the card. Though the transactions can be agreed and initiated between the parties the final settlement can be postponed to the second or third day while the amount is held in a transition or escrow account. On any security breach or reported incidence the payment transfer can be delayed until the case is settled or resolved. This would require higher transaction charges when human intervention is required. Laws are also required to prevent misuse of the delayed payment executed via credit and debit cards.

X. CONCLUSION

The conventional wisdom and process improvements in the card industry have made credit /debit cards a secure instrument in the hands of users. There are background fraud detections to terminal security measures which make it the first choice of users. Through this paper we have tried to emphasize the various aspects of security and it would be great if bank and financial instruments keep using the credit cards and debit cards to ensure maximum security of their hard earned money.

It is good to experiment with the new forms of payments but there would be a period of time which these new payment instruments need to mature and till then their use should be judiciously controlled. For now Banks should aggressively promote use of credit and debit cards for security reasons. If you are still not convinced about the significance of your digital footprints, try removing a negative comment from a bunch of websites and most of the times you would be unable to remove the negative comments even after spending subsequent time, talking to webmasters and taking legal action.

ACKNOWLEDGMENT

The authors wish to thank all the mentors of ICFAI University Jharkhand, Ranchi for giving me research opportunity. I would like to thank my Research Supervisor Dr. Mousumi Majumdar Vanguard Business School, Bangaluru and my Research Guide Dr. Sukanta Chandra Swain ICFAI University Jharkhand, Ranchi for their guidance and supervision.

REFERENCES

[1] Source www.annualreviews.org http://www.annualreviews.org/doi/pdf/10.1146/annurev-soc-071913-043145

[2] Source (milfordpublicschools.org) _https://sites.google.com/a/milfordpublicschools.org/digital- footprint-and-reputation/facts

[3] India's illiterate population is the largest in the world as per UNESCO report. Source (the hindu.com) _http://www.thehindu.com/news/national/indias-illiterate-population-largest-in-the-world-says-unesco-report/article5631797.ece

[4] Source http://digitalfootprintimu.weebly.com/follow-your-footprint.html for "Measure Your Footprint"and "Your Digital Footprint"

[5] Source http://en.wikipedia.org/wiki/EMV

AUTHOR

Surya Pratim Kesh is working as an Architect at Wipro. He works in API management and data virtualization space, and has more than 9 years of experience. He has got a Bachelor's degree in Computer Science and a MBA in Finance (part time). Currently he is pursuing Ph. D.(Part-Time) program at ICFAI University in Management. His research is focused on Plastic Money and Mobile Payments. He is published papers in his area of research.

https://in.linkedin.com/in/suryakesh