Summary Of My Research for Patent proposal

Objective

Enabling faster and secure method for cashless transactions through Virtual Card system , prioritising the transaction speed to 4x to complete the transaction in Less than 30 Seconds with out (One -time Password)and Giving it a more advanced approach with advanced Security.

Prospects for Research

->Increased Global Transactions

-> Increased cashless payments

-> concern for security

-> Present Model

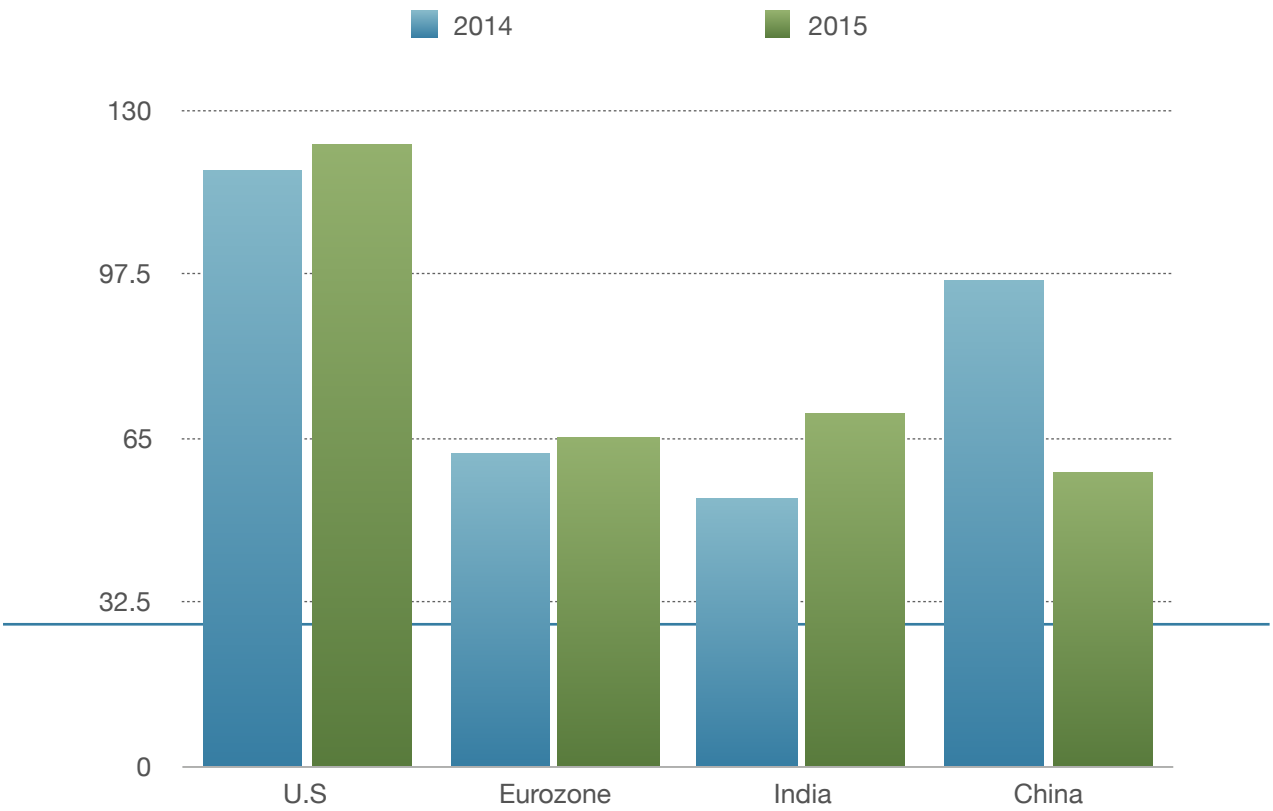
-> Proposed Model

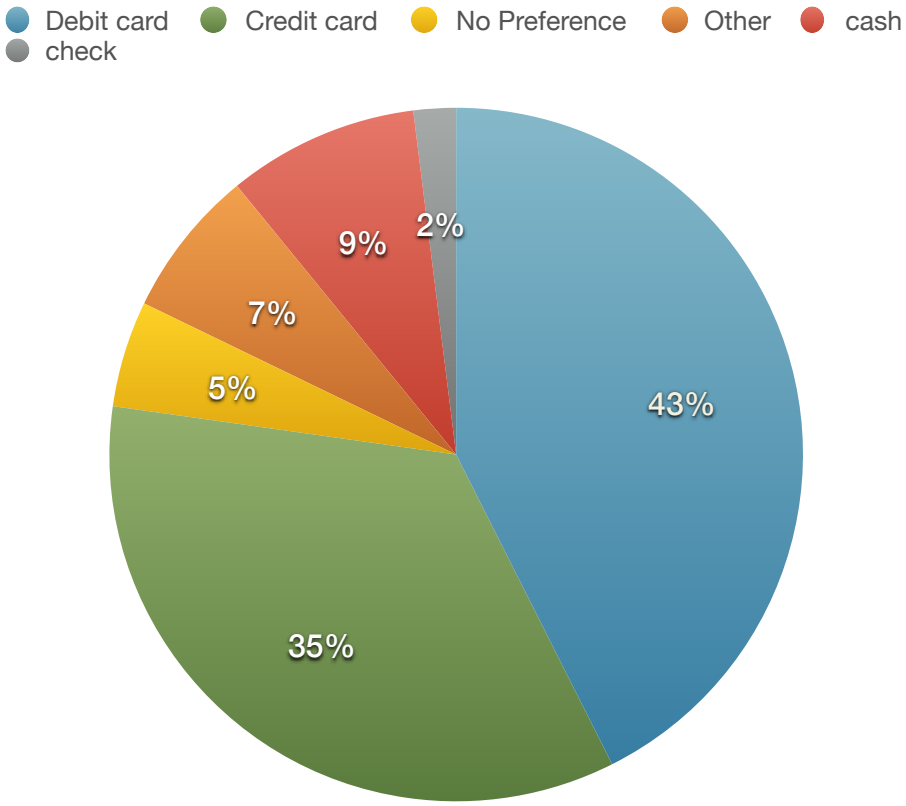
-> how this model influence the present Model

-> Present Model

-> Proposed Model

-> how this model influence the present Model





SUMMARY

INCREASED GLOBAL TRANSACTIONS - The growth Narrative for the cash less payments obtains a substantial Increase in reaching 358 billion people between 2014-15 ,Expecting a Minimum increase of 2X in the case of 2015-16.Both mature and Emerging markets Experienced the case of maximum volume growth has Put forward the Extremist research methods for Safe and faster cash less truncations .

ONLINE PAYMENTS INCREASED USAGE- Towards faster Transaction Advancements , Increased online payments make a wider approach to propose this model .

Study- Recent Stats from Wb shows that 77 % of the transactions are cashless, which happen through Mobile phone resulting in delivering the Transaction through Online cash and Subsequent Similar Methods available in various countries .

CONCERN FOR SECURITY- with all the Recent News about online Fraud and data Breach, Consumers started to Overlook their transaction process and system , This Awareness has manifested Itself in shifts in payment choices . **f**or Instance after a banking system Breach in 2015 December payments through debit card dropped upto 13 % seeking other alternatives ,During the same time a Report said that 85 % of the Credit card users fell prey for the online frauds (Financial fraud report 2015),

Which eventually dropped the use of credit cards from 85 % to 82 % . In addition there are also many other Reasons which made a shift away from debit card payment

PROSPECTS FOR MODEL-

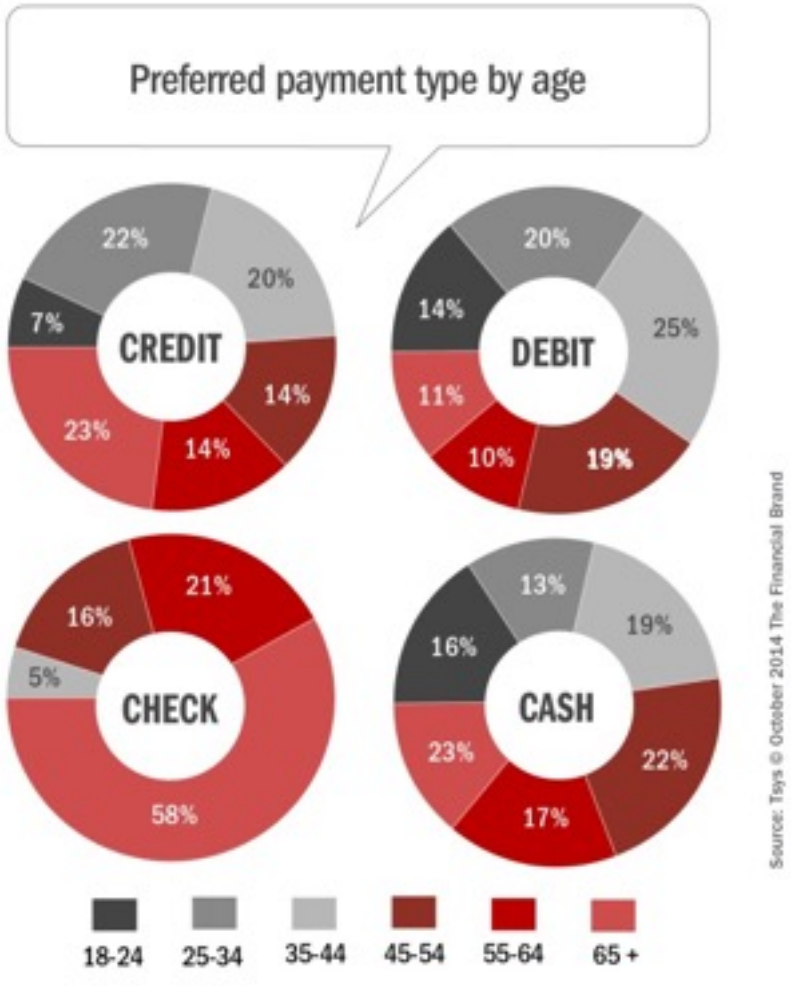
PRESENT MODEL -

This OTP is based on the very popular algorithm HMAC SHA. The HMAC SHA is an algorithm generally used to perform authentication by challenge response. It is not an encryption algorithm but a hashing algorithm that transforms a set of bytes to another set of bytes. This algorithm is not reversible which means that you cannot use the result to go back to the source

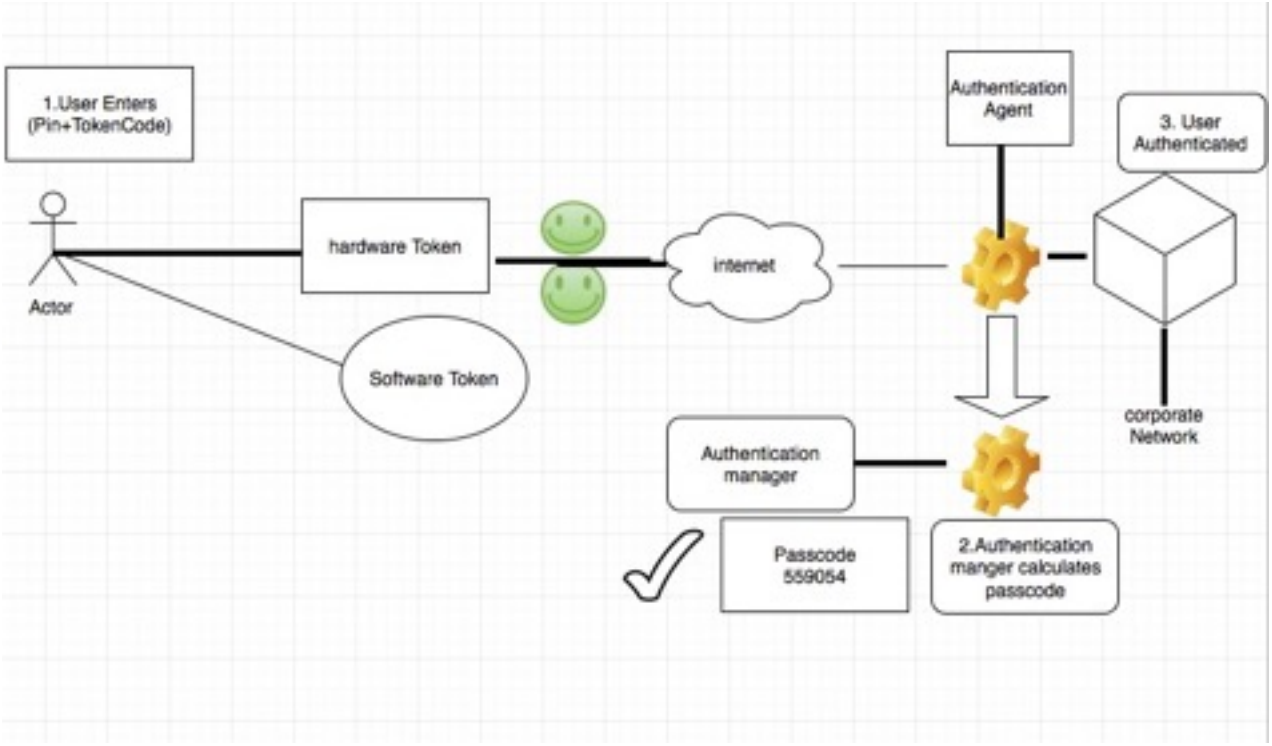
A HMAC SHA uses a key to transform an input array of bytes. The key is the secret that must never be accessible to a hacker and the input is the challenge. This means that OTP is a challenge response authentication.

The secret key must be 20 bytes at least; the challenge is usually a counter of 8 bytes which leaves quite some time before the value is exhausted.

The algorithm takes the 20 bytes key and the 8 bytes counter to create a 8 digits number. This means that there will obviously be duplicates during the life time of the OTP generator



but this doesn't matter as no duplicate can occur consecutively and an OTP is only valid for a couple of minutes.



Why OTP is Not Robustly Secure -