ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal) | |Impact Factor: 7.293||

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

Automated Teller Machine

Dr. Archana Verma

Associate Professor, Department of EAFM, BBD Govt. College, Chimanpura, Jaipur, Rajasthan, India

ABSTRACT: An automated teller machine (ATM) is an electronic telecommunications device that enables customers of financial institutions to perform financial transactions, such as cash withdrawals, deposits, funds transfers, balance inquiries or account information inquiries, at any time and without the need for direct interaction with bank staff.

ATMs are known by a variety of names, including automatic teller machines (ATM) in the United States[1][2][3] (sometimes redundantly as "ATM machine"). In Canada, the term automated banking machine (ABM) is also used,[4][5] although ATM is also very commonly used in Canada, with many Canadian organizations using ATM over ABM.[6][7][8] In British English, the terms cashpoint, cash machine and hole in the wall are most widely used.[9] Other terms include any time money, cashline, tyme machine, cash dispenser, cash corner, bankomat, or bancomat. ATMs that are not operated by a financial institution are known as "white-label" ATMs.

Using an ATM, customers can access their bank deposit or credit accounts in order to make a variety of financial transactions, most notably cash withdrawals and balance checking, as well as transferring credit to and from mobile phones. ATMs can also be used to withdraw cash in a foreign country. If the currency being withdrawn from the ATM is different from that in which the bank account is denominated, the money will be converted at the financial institution's exchange rate.[10] Customers are typically identified by inserting a plastic ATM card (or some other acceptable payment card) into the ATM, with authentication being by the customer entering a personal identification number (PIN), which must match the PIN stored in the chip on the card (if the card is so equipped), or in the issuing financial institution's database.

According to the ATM Industry Association (ATMIA), as of 2015, there were close to 3.5 million ATMs installed worldwide.[11][12] However, the use of ATMs is gradually declining with the increase in cashless payment systems.[13]

KEYWORDS-ATM,transaction, withdrawals,PIN, telecommunication,electronic

I. INTRODUCTION

The idea of out-of-hours cash distribution was first put into practice in Japan, the United Kingdom and Sweden.[14][15]

In 1960, Luther George Simjian invented an automated deposit machine (accepting coins, cash and cheques) although it did not have cash dispensing features.[16] His US patent was first filed on 30 June 1960 and granted on 26 February 1963.[17] The roll-out of this machine, called Bankograph, was delayed by a couple of years, due in part to Simjian's Reflectone Electronics Inc. being acquired by Universal Match Corporation.[18] An experimental Bankograph was installed in New York City in 1961 by the City Bank of New York, but removed after six months due to the lack of customer acceptance.[19]

In 1962 Adrian Ashfield invented the idea of a card system to securely identify a user and control and monitor the dispensing of goods or services. This was granted UK Patent 959,713 in June 1964 and assigned to Kins Developments Limited.[20]

Invention

A Japanese device called the "Computer Loan Machine" supplied cash as a three-month loan at 5% p.a. after inserting a credit card. The device was operational in 1966.[21][22] However, little is known about the device.[14]

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal) | |Impact Factor: 7.293||

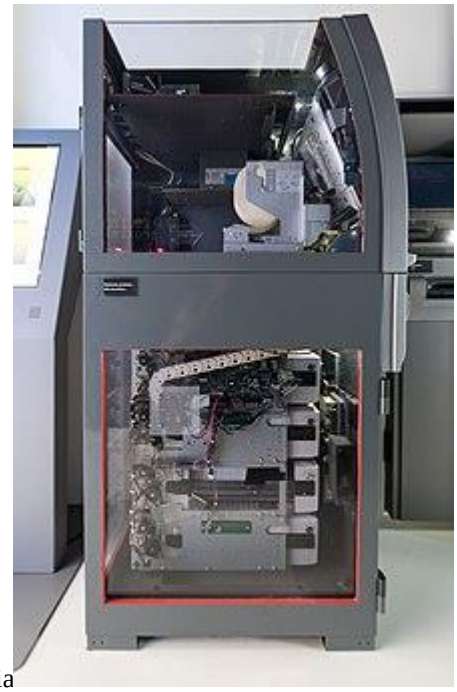
Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

A cash machine was put into use by Barclays Bank, Enfield, in the United Kingdom, on 27 June 1967, which is recognized as the world's first ATM.[23][24][25] This machine was inaugurated by English actor Reg Varney.[26] This invention is credited to the engineering team led by John Shepherd-Barron of printing firm De La Rue,[27] who was awarded an OBE in the 2005 New Year Honours.[28][29] Transactions were initiated by inserting paper cheques issued by a teller or cashier, marked with carbon-14 for machine readability and security, which in a later model were matched with a four-digit personal identification number (PIN).[27][30] Shepherd-Barron stated "It struck me there must be a way I could get my own money, anywhere in the world or the UK. I hit upon the idea of a chocolate bar dispenser, but replacing chocolate with cash."[27]

The Barclays–De La Rue machine (called De La Rue Automatic Cash System or DACS)[31] beat the Swedish saving banks' and a company called Metior's machine (a device called Bankomat) by a mere nine days and British Westminster Bank's Smith Industries Chubb system (called Chubb MD2) by a month.[32] The online version of the Swedish machine is listed to have been operational on 6 May 1968, while claiming to be the first online ATM in the world, ahead of similar claims by IBM and Lloyds Bank in 1971,[33] and Oki in 1970.[34] The collaboration of a small start-up called Speytec and Midland Bank developed a fourth machine which was marketed after 1969 in Europe and the US by the Burroughs Corporation. The patent for this device (GB1329964) was filed in September 1969 (and granted in 1973) by John David Edwards, Leonard Perkins, John Henry Donald, Peter Lee Chappell, Sean Benjamin Newcombe, and Malcom David Roe.

Both the DACS and MD2 accepted only a single-use token or voucher which was retained by the machine, while the Speytec worked with a card with a magnetic stripe at the back. They used principles including Carbon-14 and low-coercivity magnetism in order to make fraud more difficult.



Sberbank ATM in Tolyatti, Russia

Cross-section of an ATM

The idea of a PIN stored on the card was developed by a group of engineers working at Smiths Group on the Chubb MD2 in 1965 and which has been credited to James Goodfellow[35] (patent GB1197183 filed on 2 May 1966 with Anthony Davies). The essence of this system was that it enabled the verification of the customer with the debited account

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal) | |Impact Factor: 7.293||

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

without human intervention. This patent is also the earliest instance of a complete "currency dispenser system" in the patent record. This patent was filed on 5 March 1968 in the US (US 3543904) and granted on 1 December 1970. It had a profound influence on the industry as a whole. Not only did future entrants into the cash dispenser market such as NCR Corporation and IBM licence Goodfellow's PIN system, but a number of later patents reference this patent as "Prior Art Device".[25]

Propagation

Devices designed by British (i.e. Chubb, De La Rue) and Swedish (i.e. Asea Meteor) manufacturers quickly spread out. For example, given its link with Barclays, Bank of Scotland deployed a DACS in 1968 under the 'Scotcash' brand.[36] Customers were given personal code numbers to activate the machines, similar to the modern PIN. They were also supplied with £10 vouchers. These were fed into the machine, and the corresponding amount debited from the customer's account.

A Chubb-made ATM appeared in Sydney in 1969. This was the first ATM installed in Australia. The machine only dispensed $25 at a time and the bank card itself would be mailed to the user after the bank had processed the withdrawal.

1969 ABC news report on the introduction of ATMs in Sydney, Australia. People could only receive AUS $25 at a time and the bank card was sent back to the user at a later date. This was a Chubb machine.

Asea Metior's Bancomat was the first ATM installed in Spain on 9 January 1969, in central Madrid by Banesto. This device dispensed 1,000 peseta bills (1 to 5 max). Each user had to introduce a security personal key using a combination of the ten numeric buttons.[37] In March of the same year an ad with the instructions to use the Bancomat was published in the same newspaper.[38]

In West Germany, the first ATM was installed in the 50,000-people university city of Tübingen on May 27, 1968, by Kreissparkasse Tübingen. It was built by Aalen-based safe builder Ostertag AG in cooperation with AEG-Telefunken. Each of the 1,000 selected users were given a double-bit key to open the safe with "Geldausgabe" written on it, a plastic identification card, and ten punched cards. One punch card functioned as a withdrawal slip for a 100 DM bill, the maximum limit for daily use was 400 DM.[39][40]

Docutel in the United States

After looking firsthand at the experiences in Europe, in 1968 the ATM was pioneered in the U.S. by Donald Wetzel, who was a department head at a company called Docutel.[29] Docutel was a subsidiary of Recognition Equipment Inc of Dallas, Texas, which was producing optical scanning equipment and had instructed Docutel to explore automated baggage handling and automated gasoline pumps.[41]

On 2 September 1969, Chemical Bank installed a prototype ATM in the U.S. at its branch in Rockville Centre, New York. The first ATMs were designed to dispense a fixed amount of cash when a user inserted a specially coded card.[42] A Chemical Bank advertisement boasted "On Sept. 2 our bank will open at 9:00 and never close again."[43] Chemical's ATM, initially known as a Docuteller was designed by Donald Wetzel and his company Docutel. Chemical executives were initially hesitant about the electronic banking transition given the high cost of the early machines. Additionally, executives were concerned that customers would resist having machines handling their money.[44] In 1995, the Smithsonian National Museum of American History recognised Docutel and Wetzel as the inventors of the networked ATM.[45] To show confidence in Docutel, Chemical installed the first four production machines in a marketing test that proved they worked reliably, customers would use them and even pay a fee for usage. Based on this, banks around the country began to experiment with ATM installations.

By 1974, Docutel had acquired 70 percent of the U.S. market; but as a result of the early 1970s worldwide recession and its reliance on a single product line, Docutel lost its independence and was forced to merge with the U.S. subsidiary of Olivetti.[46]

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal) | |Impact Factor: 7.293||

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

In 1973, Wetzel was granted U.S. Patent # 3,761,682; the application had been filed in October 1971. However, the U.S. patent record cites at least three previous applications from Docutel, all relevant to the development of the ATM and where Wetzel does not figure, namely US Patent # 3,662,343 Archived 5 September 2017 at the Wayback Machine, U.S. Patent # 3651976 Archived 5 September 2017 at the Wayback Machine and U.S. Patent # 3,68,569 Archived 5 September 2017 at the Wayback Machine. These patents are all credited to Kenneth S. Goldstein, MR Karecki, TR Barnes, GR Chastian and John D. White.

A Chase Bank ATM in 2008

Further advances

In April 1971, Busicom began to manufacture ATMs based on the first commercial microprocessor, the Intel 4004. Busicom manufactured these microprocessor-based automated teller machines for several buyers, with NCR Corporation as the main customer.[47]

Mohamed Atalla invented the first hardware security module (HSM),[48] dubbed the "Atalla Box", a security system which encrypted PIN and ATM messages, and protected offline devices with an un-guessable PIN-generating key.[49] In March 1972, Atalla filed U.S. Patent 3,938,091 for his PIN verification system, which included an encoded card reader and described a system that utilized encryption techniques to assure telephone link security while entering personal ID information that was transmitted to a remote location for verification.[50]

He founded Atalla Corporation (now Utimaco Atalla) in 1972,[51] and commercially launched the "Atalla Box" in 1973.[49] The product was released as the Identikey. It was a card reader and customer identification system, providing a terminal with plastic card and PIN capabilities. The Identikey system consisted of a card reader console, two customer PIN pads, intelligent controller and built-in electronic interface package.[52] The device consisted of two keypads, one for the customer and one for the teller. It allowed the customer to type in a secret code, which is transformed by the device, using a microprocessor, into another code for the teller.[53] During a transaction, the customer's account number was read by the card reader. This process replaced manual entry and avoided possible key stroke errors. It allowed users to replace traditional customer verification methods such as signature verification and test questions with a secure PIN system.[52] The success of the "Atalla Box" led to the wide adoption of hardware security modules in ATMs.[54] Its PIN verification process was similar to the later IBM 3624.[55] Atalla's HSM products protect 250 million card transactions every day as of 2013,[51] and secure the majority of the world's ATM transactions as of 2014.[48]

The IBM 2984 was a modern ATM and came into use at Lloyds Bank, High Street, Brentwood, Essex, the UK in December 1972. The IBM 2984 was designed at the request of Lloyds Bank. The 2984 Cash Issuing Terminal was a true ATM, similar in function to today's machines and named Cashpoint by Lloyds Bank. Cashpoint is still a registered trademark of Lloyds Banking Group in the UK but is often used as a generic trademark to refer to ATMs of all UK banks. All were online and issued a variable amount which was immediately deducted from the account. A small number of 2984s were supplied to a U.S. bank. A couple of well known historical models of ATMs include the Atalla Box,[49] IBM 3614, IBM 3624 and 473x series, Diebold 10xx and TABS 9000 series, NCR 1780 and earlier NCR 770 series.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal) | |Impact Factor: 7.293||

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

The first switching system to enable shared automated teller machines between banks went into production operation on 3 February 1979, in Denver, Colorado, in an effort by Colorado National Bank of Denver and Kranzley and Company of Cherry Hill, New Jersey.[56]

In 2012, a new ATM at Royal Bank of Scotland allowed customers to withdraw cash up to £130 without a card by inputting a six-digit code requested through their smartphones.[57]

II. DISCUSSION

Location

The world's highest ATM at the Khunjerab Pass in Gilgit Baltistan, Pakistan, which is located at the height of 4,693 metres (15,397 ft) above sea level[58]

ATMs can be placed at any location but are most often placed near or inside banks, shopping centers/malls, airports, railway stations, metro stations, grocery stores, petrol/gas stations, restaurants, and other locations. ATMs are also found on cruise ships and on some US Navy ships, where sailors can draw out their pay.[59]

ATMs may be on- and off-premises. On-premises ATMs are typically more advanced, multi-function machines that complement a bank branch's capabilities, and are thus more expensive. Off-premises machines are deployed by financial institutions where there is a simple need for cash, so they are generally cheaper single-function devices. Independent ATM deployers unaffiliated with banks install and maintain white-label ATMs.

In the US, Canada and some Gulf countries, banks may have drive-thru lanes providing access to ATMs using an automobile.

In recent times, countries like India and some countries in Africa are installing solar-powered ATMs in rural areas.[60]

The world's highest ATM is located at the Khunjerab Pass in Pakistan. Installed at an elevation of 4,693 metres (15,397 ft) by the National Bank of Pakistan, it is designed to work in temperatures as low as -40-degree Celsius.[61]

Financial networks

An ATM in the Netherlands. The logos of a number of interbank networks to which it is connected are shown. PIN card logo are not placed, although this system was in use here at the time.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal) | |Impact Factor: 7.293||

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

Most ATMs are connected to interbank networks, enabling people to withdraw and deposit money from machines not belonging to the bank where they have their accounts or in the countries where their accounts are held (enabling cash withdrawals in local currency). Some examples of interbank networks include NYCE, PULSE, PLUS, Cirrus, AFFN, Interac,[62] Interswitch, STAR, LINK, MegaLink, and BancNet.

ATMs rely on the authorization of a financial transaction by the card issuer or other authorizing institution on a communications network. This is often performed through an ISO 8583 messaging system.

Many banks charge ATM usage fees. In some cases, these fees are charged solely to users who are not customers of the bank that operates the ATM; in other cases, they apply to all users.

In order to allow a more diverse range of devices to attach to their networks, some interbank networks have passed rules expanding the definition of an ATM to be a terminal that either has the vault within its footprint or utilises the vault or cash drawer within the merchant establishment, which allows for the use of a scrip cash dispenser.


A Diebold 1063ix with a dial-up modem visible at the base

ATMs typically connect directly to their host or ATM Controller on either ADSL or dial-up modem over a telephone line or directly on a leased line. Leased lines are preferable to plain old telephone service (POTS) lines because they require less time to establish a connection. Less-trafficked machines will usually rely on a dial-up modem on a POTS line rather than using a leased line, since a leased line may be comparatively more expensive to operate compared to a POTS line. That dilemma may be solved as high-speed Internet VPN connections become more ubiquitous. Common lower-level layer communication protocols used by ATMs to communicate back to the bank include SNA over SDLC, TC500 over Async, X.25, and TCP/IP over Ethernet.

In addition to methods employed for transaction security and secrecy, all communications traffic between the ATM and the Transaction Processor may also be encrypted using methods such as SSL.[63]

Global use

There are no hard international or government-compiled numbers totaling the complete number of ATMs in use worldwide. Estimates as of 2015 developed by ATMIA placed the number of ATMs in use at 3 million units, or approximately 1 ATM per 3,000 people in the world.[64][65]

To simplify the analysis of ATM usage around the world, financial institutions generally divide the world into seven regions, based on the penetration rates, usage statistics, and features deployed. Four regions (USA, Canada, Europe, and Japan) have high numbers of ATMs per million people.[66][67] Despite the large number of ATMs, there is additional demand for machines in the Asia/Pacific area as well as in Latin America.[68][69] Macau may have the highest density of ATMs at 254 ATMs per 100,000 adults.[70]

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

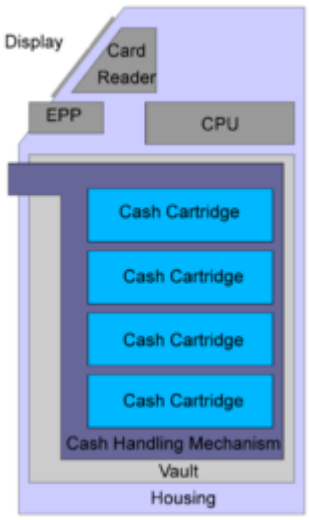
(A High Impact Factor, Monthly, Peer Reviewed Journal) | |Impact Factor: 7.293||

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

With the uptake of cashless payment solutions in the late 2010s, ATM numbers and usage started to decline. This happened first in developed countries at a time when ATM number were still increasing in Asia and Africa. As of 2013, there had been a global decline in the number of ATMs in use, with the average dropping to 39 per 100,000 adults from a peak of 41 per 100,000 adults in 2013.[13][71]

Hardware



A block diagram of an ATM

An ATM is typically made up of the following devices:

- CPU (to control the user interface and transaction devices)
- Magnetic or chip card reader (to identify the customer)
- a PIN pad for accepting and encrypting personal identification number EPP4 (similar in layout to a touch tone or calculator keypad), manufactured as part of a secure enclosure
- Secure cryptoprocessor, generally within a secure enclosure
- Display (used by the customer for performing the transaction)
- Function key buttons (usually close to the display) or a touchscreen (used to select the various aspects of the transaction)
- Record printer (to provide the customer with a record of the transaction)
- Vault (to store the parts of the machinery requiring restricted access)
- Housing (for aesthetics and to attach signage to)
- Sensors and indicators

Due to heavier computing demands and the falling price of personal computer–like architectures, ATMs have moved away from custom hardware architectures using microcontrollers or application-specific integrated circuits and have adopted the hardware architecture of a personal computer, such as USB connections for peripherals, Ethernet and IP communications, and use personal computer operating systems.

Business owners often lease ATMs from service providers. However, based on the economies of scale, the price of equipment has dropped to the point where many business owners are simply paying for ATMs using a credit card.

New ADA voice and text-to-speech guidelines imposed in 2010, but required by March 2012[72] have forced many ATM owners to either upgrade non-compliant machines or dispose them if they are not upgradable, and purchase new

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal) | |Impact Factor: 7.293||

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

compliant equipment. This has created an avenue for hackers and thieves to obtain ATM hardware at junkyards from improperly disposed decommissioned machines.[73]

 Two Loomis employees refilling an ATM at the Downtown Seattle REI

The vault of an ATM is within the footprint of the device itself and is where items of value are kept. Scrip cash dispensers, which print a receipt or scrip instead of cash, do not incorporate a vault.

Mechanisms found inside the vault may include:

- Dispensing mechanism (to provide cash or other items of value)
- Deposit mechanism including a cheque processing module and bulk note acceptor (to allow the customer to make deposits)
- Security sensors (magnetic, thermal, seismic, gas)
- Locks (to control access to the contents of the vault)
- Journaling systems; many are electronic (a sealed flash memory device based on in-house standards) or a solid-state device (an actual printer) which accrues all records of activity including access timestamps, number of notes dispensed, etc. This is considered sensitive data and is secured in similar fashion to the cash as it is a similar liability.

ATM vaults are supplied by manufacturers in several grades. Factors influencing vault grade selection include cost, weight, regulatory requirements, ATM type, operator risk avoidance practices and internal volume requirements.[74] Industry standard vault configurations include Underwriters Laboratories UL-291 "Business Hours" and Level 1 Safes,[75] RAL TL-30 derivatives,[76] and CEN EN 1143-1 - CEN III and CEN IV.[77][78]

ATM manufacturers recommend that a vault be attached to the floor to prevent theft,[79] though there is a record of a theft conducted by tunnelling into an ATM floor.[80]

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal) | |Impact Factor: 7.293||

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

Software

Although Microsoft discontinued support for the operating system in 2014, a significant number of ATMs as of 2013 still use versions of Windows XP, as seen with this machine at a branch of Tesco Express in Slough, Berkshire.

With the migration to commodity Personal Computer hardware, standard commercial "off-the-shelf" operating systems and programming environments can be used inside of ATMs. Typical platforms previously used in ATM development include RMX or OS/2.

A Wincor Nixdorf ATM running Windows 2000 (system screen removed due to copyright infringement)

Today, the vast majority of ATMs worldwide use Microsoft Windows. In early 2014, 95% of ATMs were running Windows XP.[81] A small number of deployments may still be running older versions of the Windows OS, such as Windows NT, Windows CE, or Windows 2000, even though Microsoft still supports only Windows 10 and Windows 11.

There is a computer industry security view that general public desktop operating systems have greater risks as operating systems for cash dispensing machines than other types of operating systems like (secure) real-time operating systems (RTOS). RISKS Digest has many articles about ATM operating system vulnerabilities.[82]

Linux is also finding some reception in the ATM marketplace. An example of this is Banrisul, the largest bank in the south of Brazil, which has replaced the MS-DOS operating systems in its ATMs with Linux. Banco do Brasil is also migrating ATMs to Linux. Indian-based Vortex Engineering is manufacturing ATMs that operate only with Linux. Common application layer transaction protocols, such as Diebold 91x (911 or 912) and NCR NDC or NDC+ provide emulation of older generations of hardware on newer platforms with incremental extensions made over time to address new capabilities, although companies like NCR continuously improve these protocols issuing newer versions (e.g. NCR's AANDC v3.x.y, where x.y are subversions). Most major ATM manufacturers provide software packages that implement these protocols. Newer protocols such as IFX have yet to find wide acceptance by transaction processors.[83]

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal) | |Impact Factor: 7.293||

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

With the move to a more standardised software base, financial institutions have been increasingly interested in the ability to pick and choose the application programs that drive their equipment. WOSA/XFS, now known as CEN XFS (or simply XFS), provides a common API for accessing and manipulating the various devices of an ATM. J/XFS is a Java implementation of the CEN XFS API.

While the perceived benefit of XFS is similar to the Java's "write once, run anywhere" mantra, often different ATM hardware vendors have different interpretations of the XFS standard. The result of these differences in interpretation means that ATM applications typically use a middleware to even out the differences among various platforms.

With the onset of Windows operating systems and XFS on ATMs, the software applications have the ability to become more intelligent. This has created a new breed of ATM applications commonly referred to as programmable applications. These types of applications allows for an entirely new host of applications in which the ATM terminal can do more than only communicate with the ATM switch. It is now empowered to connected to other content servers and video banking systems.

Notable ATM software that operates on XFS platforms include Triton PRISM, Diebold Agilis EmPower, NCR APTRA Edge, Absolute Systems AbsoluteINTERACT, KAL Kalignite Software Platform, Phoenix Interactive VISTAatm, Wincor Nixdorf ProTopas, Euronet EFTS and Intertech inter-ATM.

With the move of ATMs to industry-standard computing environments, concern has risen about the integrity of the ATM's software stack.[84]

Impact on labor

The number of tellers in the United States increased from approximately 300,000 in 1970 to approximately 600,000 in 2010. A contributing factor may have been the introduction of automated teller machines. ATMs allow a branch to operate with fewer tellers, making it more economical for banks to open more branches, necessitating more tellers to staff those additional branches. Further automation and online banking, however, may reverse this increase resulting in a trend toward fewer bank teller positions. [3][85]

III. RESULTS

Security

Security, as it relates to ATMs, has several dimensions. ATMs also provide a practical demonstration of a number of security systems and concepts operating together and how various security concerns are addressed.

Physical

A Wincor Nixdorf Procash 2100xe Frontload that was opened with an angle grinder

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal) | |Impact Factor: 7.293||

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

Early ATM security focused on making the terminals invulnerable to physical attack; they were effectively safes with dispenser mechanisms. A number of attacks resulted, with thieves attempting to steal entire machines by ram-raiding.[86] Since the late 1990s, criminal groups operating in Japan improved ram-raiding by stealing and using a truck loaded with heavy construction machinery to effectively demolish or uproot an entire ATM and any housing to steal its cash.

Another attack method, plofkraak, is to seal all openings of the ATM with silicone and fill the vault with a combustible gas or to place an explosive inside, attached, or near the machine. This gas or explosive is ignited and the vault is opened or distorted by the force of the resulting explosion and the criminals can break in.[87] This type of theft has occurred in the Netherlands, Belgium, France, Denmark, Germany, Australia,[88][89] and the United Kingdom.[90] These types of attacks can be prevented by a number of gas explosion prevention devices also known as gas suppression system. These systems use explosive gas detection sensor to detect explosive gas and to neutralise it by releasing a special explosion suppression chemical which changes the composition of the explosive gas and renders it ineffective.

Several attacks in the UK (at least one of which was successful) have involved digging a concealed tunnel under the ATM and cutting through the reinforced base to remove the money.[80]

Modern ATM physical security, per other modern money-handling security, concentrates on denying the use of the money inside the machine to a thief, by using different types of Intelligent Banknote Neutralisation Systems.

A common method is to simply rob the staff filling the machine with money. To avoid this, the schedule for filling them is kept secret, varying and random. The money is often kept in cassettes, which will dye the money if incorrectly opened.

Transactional secrecy and integrity

The security of ATM transactions relies mostly on the integrity of the secure cryptoprocessor: the ATM often uses general commodity components that sometimes are not considered to be "trusted systems".

Encryption of personal information, required by law in many jurisdictions, is used to prevent fraud. Sensitive data in ATM transactions are usually encrypted with DES, but transaction processors now usually require the use of Triple DES.[91][needs update] Remote Key Loading techniques may be used to ensure the secrecy of the initialisation of the encryption keys in the ATM. Message Authentication Code (MAC) or Partial MAC may also be used to ensure messages have not been tampered with while in transit between the ATM and the financial network.

Customer identity integrity

A BTMU ATM with a palm scanner (to the right of the screen)

There have also been a number of incidents of fraud by man-in-the-middle attacks, where criminals have attached fake keypads or card readers to existing machines. These have then been used to record customers' PINs and bank card information in order to gain unauthorised access to their accounts. Various ATM manufacturers have put in place countermeasures to protect the equipment they manufacture from these threats.[92][93]

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal) | |Impact Factor: 7.293||

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

Alternative methods to verify cardholder identities have been tested and deployed in some countries, such as finger and palm vein patterns,[94] iris, and facial recognition technologies. Cheaper mass-produced equipment has been developed and is being installed in machines globally that detect the presence of foreign objects on the front of ATMs, current tests have shown 99% detection success for all types of skimming devices.[95]

Device operation integrity

ATMs that are exposed to the outside must be vandal- and weather-resistant.

Openings on the customer side of ATMs are often covered by mechanical shutters to prevent tampering with the mechanisms when they are not in use. Alarm sensors are placed inside ATMs and their servicing areas to alert their operators when doors have been opened by unauthorised personnel.

To protect against hackers, ATMs have a built-in firewall. Once the firewall has detected malicious attempts to break into the machine remotely, the firewall locks down the machine.

Rules are usually set by the government or ATM operating body that dictate what happens when integrity systems fail. Depending on the jurisdiction, a bank may or may not be liable when an attempt is made to dispense a customer's money from an ATM and the money either gets outside of the ATM's vault, or was exposed in a non-secure fashion, or they are unable to determine the state of the money after a failed transaction.[96] Customers often commented that it is difficult to recover money lost in this way, but this is often complicated by the policies regarding suspicious activities typical of the criminal element.[97]

Customer security

Dunbar armored personnel watching over ATMs that have been installed in a van

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal) | |Impact Factor: 7.293||

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

In some countries, multiple security cameras and security guards are a common feature.[98] In the United States, The New York State Comptroller's Office has advised the New York State Department of Banking to have more thorough safety inspections of ATMs in high crime areas.[99]

Consultants of ATM operators assert that the issue of customer security should have more focus by the banking industry;[100] it has been suggested that efforts are now more concentrated on the preventive measure of deterrent legislation than on the problem of ongoing forced withdrawals.[101]

At least as far back as 30 July 1986, consultants of the industry have advised for the adoption of an emergency PIN system for ATMs, where the user is able to send a silent alarm in response to a threat.[102] Legislative efforts to require an emergency PIN system have appeared in Illinois,[103] Kansas[104][105] and Georgia,[106] but none has succeeded yet. In January 2009, Senate Bill 1355 was proposed in the Illinois Senate that revisits the issue of the reverse emergency PIN system.[107] The bill is again supported by the police and opposed by the banking lobby.[108]

In 1998, three towns outside Cleveland, Ohio, in response to an ATM crime wave, adopted legislation requiring that an emergency telephone number switch be installed at all outdoor ATMs within their jurisdiction. In the wake of a homicide in Sharon Hill, Pennsylvania, the city council passed an ATM security bill as well.

In China and elsewhere, many efforts to promote security have been made. On-premises ATMs are often located inside the bank's lobby, which may be accessible 24 hours a day. These lobbies have extensive security camera coverage, a courtesy telephone for consulting with the bank staff, and a security guard on the premises. Bank lobbies that are not guarded 24 hours a day may also have secure doors that can only be opened from outside by swiping the bank card against a wall-mounted scanner, allowing the bank to identify which card enters the building. Most ATMs will also display on-screen safety warnings and may also be fitted with convex mirrors above the display allowing the user to see what is happening behind them.

As of 2013, the only claim available about the extent of ATM-connected homicides is that they range from 500 to 1,000 per year in the US, covering only cases where the victim had an ATM card and the card was used by the killer after the known time of death.[109]

Jackpotting

The term jackpotting is used to describe one method criminals utilize to steal money from an ATM. The thieves gain physical access through a small hole drilled in the machine. They disconnect the existing hard drive and connect an external drive using an industrial endoscope. They then depress an internal button that reboots the device so that it is now under the control of the external drive. They can then have the ATM dispense all of its cash.[110]

Encryption

In recent years, many ATMs also encrypt the hard disk. This means that actually creating the software for jackpotting is more difficult, and provides more security for the ATM.

Uses

ATMs were originally developed as cash dispensers, and have evolved to provide many other bank-related functions:

- Paying routine bills, fees, and taxes (utilities, phone bills, social security, legal fees, income taxes, etc.)
- Printing or ordering bank statements
- Updating passbooks
- Cash advances
- Cheque Processing Module
- Paying (in full or partially) the credit balance on a card linked to a specific current account.
- Transferring money between linked accounts (such as transferring between accounts)

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal) | |Impact Factor: 7.293||

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

- Deposit currency recognition, acceptance, and recycling[111][112]

In some countries, especially those which benefit from a fully integrated cross-bank network (e.g.: Multibanco in Portugal), ATMs include many functions that are not directly related to the management of one's own bank account, such as:

- Loading monetary value into stored-value cards
- Adding pre-paid cell phone / mobile phone credit.
- Purchasing
  - Concert tickets
  - Gold[113]
  - Lottery tickets
  - Movie tickets
  - Postage stamps.
  - Train tickets
  - Shopping mall gift certificates.
- Donating to charities[114]

Increasingly, banks are seeking to use the ATM as a sales device to deliver pre approved loans and targeted advertising using products such as ITM (the Intelligent Teller Machine) from Aptra Relate from NCR.[115] ATMs can also act as an advertising channel for other companies.[116]*

A South Korean ATM with mobile bank port and bar code reader

However, several different ATM technologies have not yet reached worldwide acceptance, such as:

- Videoconferencing with human tellers, known as video tellers[117]
- Biometrics, where authorization of transactions is based on the scanning of a customer's fingerprint, iris, face, etc.[118][119][120]

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

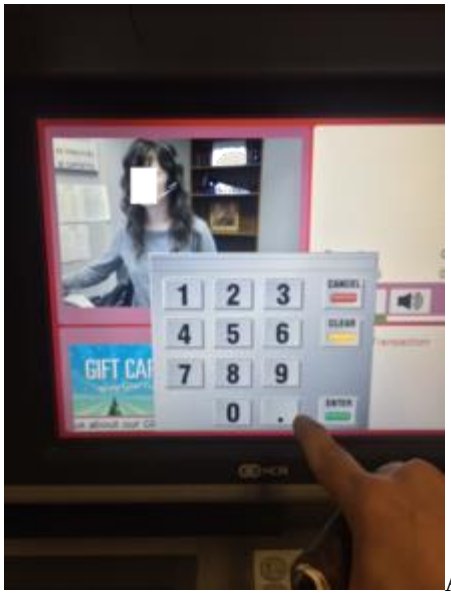
(A High Impact Factor, Monthly, Peer Reviewed Journal) | |Impact Factor: 7.293||

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

- Cheque/cash Acceptance, where the machine accepts and recognises cheques and/or currency without using envelopes[121] Expected to grow in importance in the US through Check 21 legislation.
- Bar code scanning[122]
- On-demand printing of "items of value" (such as movie tickets, traveler's cheques, etc.)
- Dispensing additional media (such as phone cards)
- Co-ordination of ATMs with mobile phones[123]
- Integration with non-banking equipment[124][125]
- Games and promotional features[126]
- CRM through the ATM

Videoconferencing teller machines are currently referred to as Interactive Teller Machines. Benton Smith writes in the Idaho Business Review, "The software that allows interactive teller machines to function was created by a Salt Lake City-based company called uGenius, a producer of video banking software. NCR, a leading manufacturer of ATMs, acquired uGenius in 2013 and married its own ATM hardware with uGenius' video software



A NCR Interactive Teller Machine running uGenius software

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal) | |Impact Factor: 7.293||

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

- Pharmacy dispensing units[128]

Reliability

An ATM running Microsoft Windows that has crashed due to a peripheral component failure

Before an ATM is placed in a public place, it typically has undergone extensive testing with both test money and the backend computer systems that allow it to perform transactions. Banking customers also have come to expect high reliability in their ATMs,[129] which provides incentives to ATM providers to minimise machine and network failures. Financial consequences of incorrect machine operation also provide high degrees of incentive to minimise malfunctions.[130]

ATMs and the supporting electronic financial networks are generally very reliable, with industry benchmarks typically producing 98.25% customer availability for ATMs[131] and up to 99.999% availability for host systems that manage the networks of ATMs. If ATM networks do go out of service, customers could be left without the ability to make transactions until the beginning of their bank's next time of opening hours.

This said, not all errors are to the detriment of customers; there have been cases of machines giving out money without debiting the account, or giving out higher value notes as a result of incorrect denomination of banknote being loaded in the money cassettes.[132] The result of receiving too much money may be influenced by the card holder agreement in place between the customer and the bank.[133][134]

Errors that can occur may be mechanical (such as card transport mechanisms; keypads; hard disk failures; envelope deposit mechanisms); software (such as operating system; device driver; application); communications; or purely down to operator error.

To aid in reliability, some ATMs print each transaction to a roll-paper journal that is stored inside the ATM, which allows its users and the related financial institutions to settle things based on the records in the journal in case there is a dispute. In some cases, transactions are posted to an electronic journal to remove the cost of supplying journal paper to the ATM and for more convenient searching of data.

Improper money checking can cause the possibility of a customer receiving counterfeit banknotes from an ATM. While bank personnel are generally trained better at spotting and removing counterfeit cash,[135][136] the resulting ATM money supplies used by banks provide no guarantee for proper banknotes, as the Federal Criminal Police Office of Germany has confirmed that there are regularly incidents of false banknotes having been dispensed through ATMs.[137] Some ATMs may be stocked and wholly owned by outside companies, which can further complicate this problem. Bill validation technology can be used by ATM providers to help ensure the authenticity of the cash before it is stocked in the machine; those with cash recycling capabilities include this capability.[138]

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal) | |Impact Factor: 7.293||

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

In India, whenever a transaction fails with an ATM due to network or technical issues and if the amount does not get dispensed in spite of the account being debited then the banks are supposed to return the debited amount to the customer within seven working days from the day of receipt of a complaint. Banks are also liable to pay the late fees in case of delay in repayment of funds post seven days.[139]

As with any device containing objects of value, ATMs and the systems they depend on to function are the targets of fraud. Fraud against ATMs and people's attempts to use them takes several forms.

The first known instance of a fake ATM was installed at a shopping mall in Manchester, Connecticut, in 1993. By modifying the inner workings of a Fujitsu model 7020 ATM, a criminal gang known as the Bucklands Boys stole information from cards inserted into the machine by customers.[140]

WAVY-TV reported an incident in Virginia Beach in September 2006 where a hacker, who had probably obtained a factory-default administrator password for a filling station's white-label ATM, caused the unit to assume it was loaded with US$5 bills instead of $20s, enabling himself—and many subsequent customers—to walk away with four times the money withdrawn from their accounts.[141] This type of scam was featured on the TV series The Real Hustle.

ATM behaviour can change during what is called "stand-in" time, where the bank's cash dispensing network is unable to access databases that contain account information (possibly for database maintenance). In order to give customers access to cash, customers may be allowed to withdraw cash up to a certain amount that may be less than their usual daily withdrawal limit, but may still exceed the amount of available money in their accounts, which could result in fraud if the customers intentionally withdraw more money than they had in their accounts.[142]

IV. CONCLUSIONS

Card fraud

In an attempt to prevent criminals from shoulder surfing the customer's personal identification number (PIN), some banks draw privacy areas on the floor.

For a low-tech form of fraud, the easiest is to simply steal a customer's card along with its PIN. A later variant of this approach is to trap the card inside of the ATM's card reader with a device often referred to as a Lebanese loop. When the customer gets frustrated by not getting the card back and walks away from the machine, the criminal is able to remove the card and withdraw cash from the customer's account, using the card and its PIN.

This type of fraud has spread globally. Although somewhat replaced in terms of volume by skimming incidents, a re-emergence of card trapping has been noticed in regions such as Europe, where EMV chip and PIN cards have increased in circulation.[143]

Another simple form of fraud involves attempting to get the customer's bank to issue a new card and its PIN and stealing them from their mail.[144]

By contrast, a newer high-tech method of operating, sometimes called card skimming or card cloning, involves the installation of a magnetic card reader over the real ATM's card slot and the use of a wireless surveillance camera or a modified digital camera or a false PIN keypad to observe the user's PIN. Card data is then cloned into a duplicate card and the criminal attempts a standard cash withdrawal. The availability of low-cost commodity wireless cameras, keypads, card readers, and card writers has made it a relatively simple form of fraud, with comparatively low risk to the fraudsters.[145]

In an attempt to stop these practices, countermeasures against card cloning have been developed by the banking industry, in particular by the use of smart cards which cannot easily be copied or spoofed by unauthenticated devices, and by attempting to make the outside of their ATMs tamper evident. Older chip-card security systems include the French Carte Bleue, Visa Cash, Mondex, Blue from American Express[146] and EMV '96 or EMV 3.11. The most actively developed form of smart card security in the industry today is known as EMV 2000 or EMV 4.x.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal) | |Impact Factor: 7.293||

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

EMV is widely used in the UK (Chip and PIN) and other parts of Europe, but when it is not available in a specific area, ATMs must fall back to using the easy–to–copy magnetic stripe to perform transactions. This fallback behaviour can be exploited.[147] However, the fallback option has been removed on the ATMs of some UK banks, meaning if the chip is not read, the transaction will be declined.

Card cloning and skimming can be detected by the implementation of magnetic card reader heads and firmware that can read a signature embedded in all magnetic stripes during the card production process. This signature, known as a "MagnePrint" or "BluPrint", can be used in conjunction with common two-factor authentication schemes used in ATM, debit/retail point-of-sale and prepaid card applications.

The concept and various methods of copying the contents of an ATM card's magnetic stripe onto a duplicate card to access other people's financial information were well known in the hacking communities by late 1990.[148]

In 1996, Andrew Stone, a computer security consultant from Hampshire in the UK, was convicted of stealing more than £1 million by pointing high-definition video cameras at ATMs from a considerable distance and recording the card numbers, expiry dates, etc. from the embossed detail on the ATM cards along with video footage of the PINs being entered. After getting all the information from the videotapes, he was able to produce clone cards which not only allowed him to withdraw the full daily limit for each account, but also allowed him to sidestep withdrawal limits by using multiple copied cards. In court, it was shown that he could withdraw as much as £10,000 per hour by using this method. Stone was sentenced to five years and six months in prison.[149]

Related devices

A talking ATM is a type of ATM that provides audible instructions so that people who cannot read a screen can independently use the machine, therefore effectively eliminating the need for assistance from an external, potentially malevolent source. All audible information is delivered privately through a standard headphone jack on the face of the machine. Alternatively, some banks such as the Nordea and Swedbank use a built-in external speaker which may be invoked by pressing the talk button on the keypad.[150] Information is delivered to the customer either through pre-recorded sound files or via text-to-speech speech synthesis.

A postal interactive kiosk may share many components of an ATM (including a vault), but it only dispenses items related to postage.[151][152]

A scrip cash dispenser may have many components in common with an ATM, but it lacks the ability to dispense physical cash and consequently requires no vault. Instead, the customer requests a withdrawal transaction from the machine, which prints a receipt or scrip. The customer then takes this receipt to a nearby sales clerk, who then exchanges it for cash from the till.[153]

A teller assist unit (TAU) is distinct in that it is designed to be operated solely by trained personnel and not by the general public, does integrate directly into interbank networks, and usually is controlled by a computer that is not directly integrated into the overall construction of the unit.

A Web ATM is an online interface for ATM card banking that uses a smart card reader. All the usual ATM functions are available, except for withdrawing cash. Most banks in Taiwan provide these online services.[154][155]

REFERENCES

1. Merriam-Webster Dictionary. Springfield, MA: Merriam-Webster. Archived from the original on 12 August 2017. Retrieved 7 January 2017.
2. ^ "FNSRTS307A - Maintain Automatic Teller Machine (ATM) services". training.gov.au. Archived from the original on 7 April 2014.
3. ^ Cambridge Dictionary Automatic Teller Machine Archived 7 April 2014 at the Wayback Machine
4. ^ "Interac FAQ". Interac Association. Retrieved 28 January 2017.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal) | |Impact Factor: 7.293||

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

5. ^ "Automated Banking Machine (ABM)". Scotiabank. Archived from the original on 26 November 2012.
6. ^ Financial Consumer Agency of Canada (8 June 2017). "ATM fees". Canada.ca. Archived from the original on 29 July 2017. Retrieved 29 July 2017.
7. ^ "ATM and Banking Centre Network". CIBC. Archived from the original on 29 July 2017. Retrieved 29 July 2017.
8. ^ "TD Green Machine ATM Machines". TD Canada Trust. Archived from the original on 19 July 2015. Retrieved 29 July 2017.
9. ^ Merriam-Webster Dictionary. Springfield, MA: Merriam-Webster. Archived from the original on 9 January 2017. Retrieved 7 January 2017.
10. ^ Schlichter, Sarah (5 February 2007). "Using ATM's abroad - Travel - Travel Tips". NBC News. Archived from the original on 1 March 2014. Retrieved 11 February 2011.
11. ^ "ATM Industry Association". Archived from the original on 16 October 2015.
12. ^ Morrison, David (28 July 2014). "3 Million ATMs Worldwide By 2015: ATM Association". Credit Union Times. Archived from the original on 26 June 2015.
13. ^ [a] [b] Cummins, Carolyn (1 December 2017). "Shopping centres prepare to go cashless as ATMs disappear". The Age. Archived from the original on 4 December 2017. Retrieved 27 March 2011.
14. ^ [a] [b] "A Brief History of the ATM". The Atlantic. 26 March 2015. Archived from the original on 28 April 2015. Retrieved 26 April 2015.
15. ^ Batiz-Lazo, Bernardo (27 March 2013). "How the ATM Revolutionized the Banking Business". Bloomberg. Archived from the original on 9 February 2014.
16. "ATMIA 50th Anniversary Factsheet" (PDF). www.atmia.com. ATM Industry Association. October 2015. Archived (PDF) from the original on 18 August 2016. Retrieved 29 June 2016.
17. ^ "Machine Accepts Bank Deposits", The New York Times, 12 April 1961
18. ^ US patent 3079603, Luther G Simjian, "Depository machine combined with image recording means", issued 1963-02-26
19. ^ "Universal Match Maps Acquisition", The New York Times, 22 March 1961
20. ^ "From punchcard to prestaging: 50 years of ATM innovation". ATM Marketplace. 31 July 2013. Archived from the original on 15 August 2013. Retrieved 27 September 2013.
21. ^ GB patent 959713, Adrian Walter Francis Ashfield, "Access Controller", published 1962-02-15, issued 1964-06-03, assigned to Kins Developments Ltd
22. ^ 'Fast Machine With a Buck', "Pacific Star and Stripes", 7 July 1966
23. ^ 'Instant Cash with a Credit Card', "ABA Banking Journal", January 1967
24. ^ "1967: First Cash Dispenser". Guinness World Records. 19 August 2015. Retrieved 10 April 2011.
25. ^ Murray, Amelia (25 June 2017). "The story behind the world's first cashpoint". The Telegraph. ISSN 0307-1235. Retrieved 10 April 2011; Alberge, Dalya (10 April 2011). "Bank that opened world's first ATM given heritage status". The Telegraph. ISSN 0307-1235. Retrieved 10 April 2011.
26. ^ [a] [b] Batiz-Lazo, Bernardo; Reid, Robert J. K. (30 June 2008). "Evidence from the Patent Record on the Development of Cash Dispensing Technology" (PDF). Munich Personal RePEc Archive. p. 4. Archived (PDF) from the original on 4 September 2015. Retrieved 27 April 2015.
27. ^ "Enfield's cash gift to the world". BBC London. 27 June 2007. Archived from the original on 3 November 2015.
28. ^ [a] [b] [c] Milligan, Brian (25 June 2007). "The man who invented the cash machine". BBC News. Archived from the original on 26 December 2009. Retrieved 26 April 2010.
29. ^ "ATM inventor honoured". BBC News. 31 December 2004. Archived from the original on 8 June 2010. Retrieved 26 April 2010.
30. ^ [a] [b] Harper, Tom; Batiz-Lazo, Bernardo (2013). Cash Box: The Invention and Globalization of the ATM. Networld Media Group. ISBN 978-1935497622.
31. ^ "ATM inventor John Shepherd-Barron dies at age of 84 on 20th May 2010". Los Angeles Times. 19 May 2010. Archived from the original on 23 May 2010.