Classify and Analyze the Security Issues and Challenges in Mobile banking in Uzbekistan

Azamjon Abdullaev *, Mohammed Abdulhakim Al-Absi *, Ahmed Abdulhakim Al-Absi **, Mangal Sain*, Hoon Jae Lee *

* *Dongseo University, Busan, Republic of Korea*

** *Kyungdong University Gangwon-do, Republic of Korea*

azamjon.a.sobirovich@gmail.com, mohammed.a.absi@gmail.com, absiahmed@kduniv.ac.kr, mangalsain1@gmail.com, hjlee@dongseo.ac.kr

***Abstract*—Due to advancement and growth in mobile technology, mobile banking is now included in our lives. in Uzbekistan, Mobile banking is a subset of Mobile-services where all banks provide Internet banking service uses SSL encryption of data transmitted from the user's computer to the bank system and vice versa. Security measure allows the users to exclude a previously common type of fraud. The security in crowded enterprise architecture is a concern that encompasses user's mobile clients, web applications, mobile devices, back -end applications and networks. All systems interfaces can undergo a form of attacks and it needs to be secured. The main objective of this work is to classify and analyze the Security issues and challenges in Mobile banking in Uzbekistan.**

***Keyword*—Internet banking, Mobile Banking, Challenges Mobile Banking in Uzbekistan, Security Issue.**

I. INTRODUCTION

THE internet has both the attributes and advantages that can transcend the limits of space and distance facilitating the delivery of service "anywhere at any time" from any internet-enabled device. These technological advances have enabled consumers to avail of banking services without the need to physically visit a bank. Financial institutions have also identified the opportunities these technological advances present to attract new customers, develop and maintain current customer relationships, cross-selling of products and develop new innovative service offerings.

For today, online banking is one of the modern tools, which allow banks to increase their profitability and increase their profitability client base. This article examines the world-wide issues and challenges online banking as well as an overview of the current status of online banking in Uzbekistan.

A mobile phone is a device that widespread technology that turns into a part of every person in the information era. Mobile banking is a framework that permits clients of a monetary organization to direct various budgetary exchanges through a cell phone, for example, cell phone or personal digital assistant. Mobile Banking indicates to arrangement and benefits of saving money and monetary administrations with the assistance of mobile telecommunication devices. Banking is one of the big financial foundations that explore the opportunity of technology where this technology allowed the services to have the best customer experience and comfort. Technologies perform a significant role in the banking sector. The development of mobile devices nowadays, mobile banking is one of the important strategies in the banking industry. Mobile banking is a mobile computing application which supports customers with mobile banking service. Whenever and what they want, the users be able to mobile banks such as short messages. Mobile banking [1] has emerged as a popular mode of banking in many developed and developing countries. Access to mobile data services can be a distinct part depending on technology or performance type. The current population of Uzbekistan is 32,520,015 as of Tuesday, November 6, 2018, based on the latest United Nations estimates.

Depend on the International Telecommunication Union, the number of mobile users in 2017 [2] exceeds more than 7 billion. In 2000, their number was estimated to be 1 billion. In turn; the number of Internet users reached 4.2 billion. The number of mobile subscribers in Uzbekistan has increased by 1.4 million in 2017 compared to 2016 and amounted to 22.8 million people in January 2018.

Nowadays, internet banking helps the users and customers.

Manuscript received on Jan. 1, 2019. This work was supported by the Institute for Information and Communications Technology Promotion (Grant Number: 2018-0-00245) and it was also supported by the Basic Science Research Program through the National Research Foundation of Korea funded by the Ministry of Education, Science, and Technology (Grant Number: NRF2016R1D1A1B01011908), and a follow-up of the invited journal to the accepted & presented paper entitled "Security Challenge and Issue of Mobile Banking in Republic of Uzbekistan: A State of Art Survey" of the 21th International Conference on Advanced Communication Technology (ICACT2019).

Azamjon Abdullaev. Currently, he is a Master student in the Department of Computer Engineering at Dongseo University, South Korea. (e-mail: azamjon.a.sobirovich@gmail.com)

Mohammed Abdulhakim Al-Absi. Currently, he is a Ph.D. student in the Department of Computer Engineering at Dongseo University, South Korea. (e-mail: mohammed.a.absi@gmail.com)

Ahmed Abdulhakim Al-Absi. Author is an assistant professor and head of smart computing department at Kyungdong University - Global Campus in South Korea. (e-mail: absiahmed@kduniv.ac.kr)

Mangal Sain. Author is an Assistant Professor in the Department of Computer Engineering, Dongseo University, South Korea. (e-mail: mangalsain1@gmail.com)

Hoon Jae Lee. Currently, he is a professor in the Department of Information Communication Engineering at Dongseo University, South Korea (corresponding author, phone: +82-10-2801-3735, email: hjlee@dongseo.ac.kr)

Customers can money transfer, check out their account details, get their bank account statements and pay money sitting in the comfort of their offices and at home. On the other hand, the biggest limitation of internet banking needs a personal computer and internet connection. And this is a little problem in developing countries if we consider most developing countries especially in Uzbekistan. Despite various initiatives, the level of internet connection in Uzbekistan is still relatively low. Mobile banking can solve this problem as it reduces the user's requirement to just their mobile phones.

Payments for all mobile services in Uzbekistan (Ucell, UzMobile CDMA, UzMobile GSM, UMS, Beeline, Perfectum); Natural gas and electricity payments; Internet access charges (Sarkor Telecom, Uzonline, EVO, TPS); Payments for fixed telephony; Payments for IPTV; Payments for cable television (UzDigital TV, Stars TV); [3] Payments within the system, Customers can transfer funds from plastic card through the special account opened to them by transferring funds from other plastic cards to the mobile bank's special number, i.e. non-cash Payments; Individuals Monthly payments for loans received from Bank branches; One - time payments for goods and services purchased.

II. MOBILE PAYMENT CHARACTERISTICS

In developing countries for example in Uzbekistan, mobile banking providers rely on agents to acquire customers and manage liquidity. They reach sensitive customer information such as the mobile number, user name, and other credentials used for authentication and identification purpose. These factors are not well equipped to keep customer sensitive information and can be easily lead to information leakage. The failure of a service provider to protect or control sensitive information is a serious threat to business processes and potential customer security.

There are some conditions for the mobile payment service to be acceptable as a market payment service:

- Universality: where the mobile banking should give transactions services among Business to Businesses (B2B), Customer to Customer (C2C), and Businesses to Customer (B2C)
- Interoperability: combining technologies as one system based on standards
- Security, Privacy and Trust: customers go to the bank and give their personal information and also depositing their money. However, there should be trust between the customer and the bank so the customer can trust the mobile banking payment service and make sure that his personal information not be misused.
- Simplicity and Usability: mobile banking payment services should able to fit the customer's convenience.
- Cross border payments: mobile banking should be widely accepted in the word-wide
- Cost and Speed: where speed it's very important in the mobile payment that convenience merchants and customers.

III. BANKING SYSTEM AND MOBILE BANKING IN UZBEKISTAN

Uzbekistan has 29 commercial banks, including 5 state-owned banks, 13 state-owned banks, 5 foreign banks, and 6 private banks. There are 8,610 credit institutions nationwide, including microfinance institutions and commercial bank branches. The Uzbek banking system remains under State control through a series of regulatory measures, legislation, declarations and complex practices. Most bank assets are still in state-owned or state-controlled banks, and most of the loans are directed by the government or directed to develop a pre-determined industrial sector. By limiting the role of banks as a financial intermediary to reform the slow financial system, it limits the ability of citizens and private companies to access credit and other financial services [21].

Mobile banking in Uzbekistan, primarily by Hamkorbank and its international financial corporation and the Asian Development Bank, was developed by a hamkormobile platform in May 2009 [4]. It was an independent platform allowing operators to save, receive, transfer, withdraw money, as well as buy goods and services.

Remote service for individuals - this is a system that allows you to control your bank account from anywhere using a mobile phone or the Internet browser [5].

IV. SYSTEM OPPORTUNITIES

Payments for cellular operators and fixed telephony, Internet providers and digital television services, Utility payments, Single-time payments for Consumer Goods and Services, and other payments, payments for consumer and mortgage loans, seeing and replenishing of account status, obtaining information on deposit balances and interest accrued, online Smart Visa balances and its get information about turnover [6]. Payments to the budget, transfer of bonus cards from card to card, online conversion, connecting Visa and Union Pay cards and checking account status and more.

We can see from Table I [20], three banks controlled 59.9% of the total assets banking in 2018 compared to 86.9% in 2001. The National Bank of Uzbekistan controlled 76% of the banking sector in 2001 where 30.9% in January 2018. The national bank of Uzbekistan controlling 19.5% and 18.5% of the deposit and market loan shares in 2018. The foreign ownership controlled 7.7% of the sector in 2018. However, there is 0.8% of the share of the bank with no state ownership is increased in 2001 to 13% in 2018.

TABLE I
UZBEKISTAN'S BANKING SYSTEM OWNERSHIP AND CONCENTRATION

Market Share (Percentage of Banking Assets)				
	2001	2014	2016	2018
Market share of the top three banks	86.6	50.6	49.7	59.9
Market share of the top five banks	91.3	63.7	62.9	71.8
State-owned banks	82.2	41.2	41.4	48.8

Shareholding banks with indirect state ownership	6.1	35.5	33.7	33.2
Banks with foreign ownership	0.9	8.7	9.9	7.7

The main provider mobile platform in Uzbekistan CLICK was founded in November 2011. The activity of the company is the development of software products for commercial banks, organizations, individuals, their adaptation to various hardware and software complexes and further improvement. software products are protected by the current legislation of the Republic of Uzbekistan [7]. "CLICK" system is a mobile banking system that allows mobile operators to pay for services of cellular operators, Internet providers and other companies; traditional and internet-shop purchases, card-to-card transfers, and more. Key features of the CLICK system:

- transfer from card to card
- "CLICK Terminal" service
- Manage the accounts you have sent to you
- Auto payment service
- View payment history
- An online check of account balances
- Repayment of received loans
- SMS notifications

The advantages of the click system are as follows; Hammerliness: Usage of a USSD-request on a negative balance and without the use of the Internet, even if the user's number is blocked, can pay at any time from his bank account. In order to use the system, you do not need to install any software on the phone: USSD-request can be sent from any mobile phone [8].

Proximity: Opportunity to replenish the balance and manage your bank account, without having to go to the bank branches and paying for the recent payment receipt or payment acceptance and payment system locations opportunity to pay without leaving home. The entire payment system is in the pocket of each subscriber.

In order to connect to the system, it is not required to open special accounts in the bank and deposit funds to another deposit. Our system allows you to "bind" your number to any existing account of an individual.

V. SECURITY ISSUES AND CHALLENGES IN MOBILE BANKING

Mobile banking has become a big challenge for banks because of the fast development of mobile technologies such as 1G, 2G, 3G, 4G, and 5G. In Uzbekistan, most of people use the ATM machine as well as online banking services. However, they are afraid of mobile banking due to the theft of mobile handset and misuse.

A. Security issues and Mobile banking with Wireless Application Protocol

New technology has made people access to the internet much easier. Users connect their mobile devices to WAP and GPRS, access various banking services, such as transferring money from one account to another and paying the cost of items purchased. In Uzbekistan, mobile devices have become widespread and are becoming necessary for consumers, entrepreneurs and business people alike. Although these devices are relatively small and inexpensive but have multiple features. Portable devices have built-in special devices, such as accelerometers, cameras, removable media readers and GPS receivers. It also integrates many wireless technologies such as Wireless Fidelity (Wi-Fi), Bluetooth, Near Field Connection (NFC) and Mobile Interface (CDMA or GSM). The interconnect network is connected to the world. At the same time, security and convenience are important factors in the growth of mobile banking and mobile device trading.

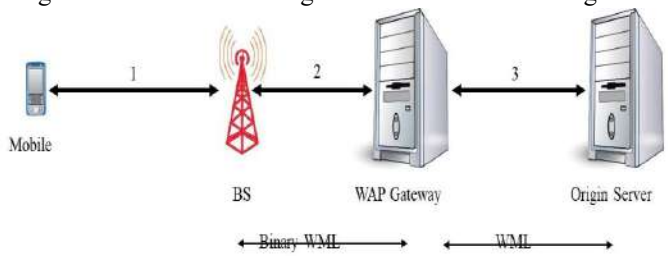

Fig. 1. Security aspect in the WAP architecture

Wireless Application Protocol is used for communication among devices where the customer uses it to realize the functionality of internet banking. For secure and successful transmission between the customer and bank, the encryption data process has been used but this is not good enough to secure the sensitive data among the customer and bank. The transmission needs to be more security methods with high memory storage capacity. We are unable to apply a complex cryptographic systems due to the mobiles have a low computational capacity [9]. Table II shows the Security threads for mobile banking.

Because of the technology development is increasing day by day, it is important to provide very good end-to-end security Fig. 1. However, it is very difficult to provide security using WAP because at the gateway the data is not encrypted while switching of protocol process [10]

There are two technologies are using for mobile banking namely Wireless Internet Gateway (WIG) (short message service) and Wireless Application Protocol (WAP). Security is very important before you provide the services [11]

TABLE II
SECURITY THREADS FOR MOBILE BANKING

Danger Identification regarding Mobile banking	
Security threads for mobile banking	Security issues and Mobile banking with Wireless Application Protocol
	Transaction and massage transmission Using mobile Banking
	Third-party identification password
	Identification of password

Recently in Uzbekistan that banks had a chance long enough to communicate with customer's mobile banking applications so and with their performers - the developers, so they are able to look at problems from different positions. Often there are organizational problems when in their

technical assignments for customers. The problem of data storage, Mobile devices can be easily lost or just lose sight for a while. Meanwhile, they can say about their owners much more than their board "brothers". Therefore, the problem of data storage on mobile devices is one of the most important. When analyzing the security of mobile applications banking often observes critical information in open form, which is either simply stored in the application, or unconsciously "falls" in cache network requests, logs, crash dumps, screenshots. An attacker when getting physical access, the device can download these critical files. Another equally important issue is to work in an untrusted environment. Often users put themselves their devices are at risk getting root access on their Android device or installing jailbreak on iOS devices. However, they often do not understand that when you receive various free "bonuses" The OS's built-in security mechanisms are partially or completely disabled. This increases the probability of infection of the device with malicious code and implements a successful attack by an attacker. Worth noting is the problem of application distribution. It concerns only mobile operating systems with many app stores, and first of all, the Android OS. For Android, there is a huge number of stores (Google Play, Samsung Apps, Yandex market, Amazon mobile app distribution, Slide Me, etc.). Some of them are installed by default. As a result, one store may contain the legitimate application, and in another - its modified version with malicious functionality.

There are also unofficial applications for banks that often represent "Wrappers" over Internet sites. We recommend use only official apps, but banks need to monitor store applications to detect fakes.

Code deobfuscation occurs in Android applications. In IOS, it is absolutely missing. The situation is similar with anti-debug technicians as for channel security data transfer. This is a problem for mobile banking. But mobile devices are good that provides freedom of movement and choosing a place to connect to the network on your own.

B. Authentication Risks and Issues

The people like to use the mobile phone anywhere they go so they use the mobile banking application while they are moving and in any situation. The Security mechanism can be done by identifying the customer's pin number, phone number etc.

Authentication Model: two kinds of services are provided to the customer's one is the direct bank services to the customer and the second one is the bank will share the services to the third-party provider.

C. Bank provides the service directly to the customer Architecture

If a customer wants to transfer money using mobile banking he has to authenticate himself to the bank sever using a firewall then the server will verify the customer security password and pin number then the bank will allow him to complete the process for money transfer[12]. This method has security issues for instance system crash, server failure and malevolent intrusion [13]. However, banks don't prefer using this method Fig. 2.

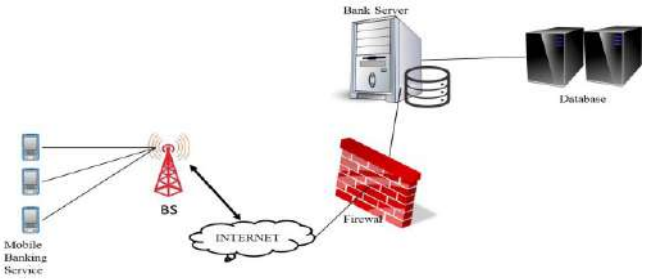

Fig. 2. Service directly to customer Architecture

D. SMS Spoofing Attack

The spoofing attack is the most serious attack in SMS mobile banking where the attacker can send a message to the sender number so most of the organism doesn't use mobile banking using SMS [14]

E. Mobile banking virus attacks

There are many types of viruses, Trojan and malicious internet program [15]. For instance, Trojan can get the password from the web easily and from the operating system cached information. Zeus Trojan is used for stealing the password and the authentication number for the mobile banking transactions [16]

VI. MOBILE PAYMENT SECURITY FRAMEWORK

In fact, mobile phone payments can be divided into payments close to the field and remote payments. Near-field payments include an RFID-based mobile payment framework and an NFC-based mobile payment framework. Payment is not yet popular and is limited. In the case of a request, the protection of unencrypted information is not yet effective. In addition, some attackers convert NFC-enabled mobile phones to point-of-sale (POS) devices for non-contact card transactions as well as point-of-sale (POS) frauds in Portuguese phone mode.

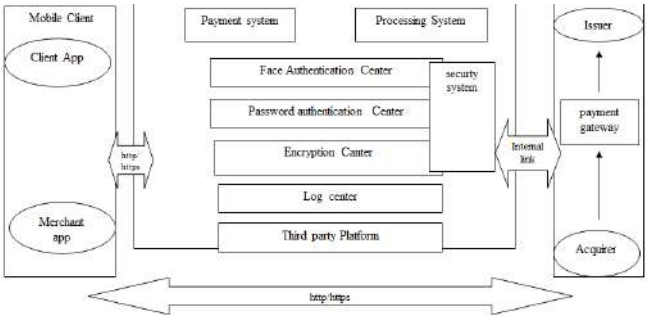

Fig. 3. The framework consists of three parts: a transaction interface, a server-side and a mobile client.

Mobile Client: The application appears in the client application and sales application in Fig. 3 because the application needs to complete the user's work. The two applications use the same program structure as they are used to perform the payment.

VII. INTERFACES DESIGN AND MOBILE PAYMENT SECURITY PROCESSES

This frame adds the idea of face recognition to secure user accounts. At the same time, a third-party regulatory body has been added to manage the user's assets. If the user logs on to

the system using Uname and Psd, the payment process is as follows Fig. 4:

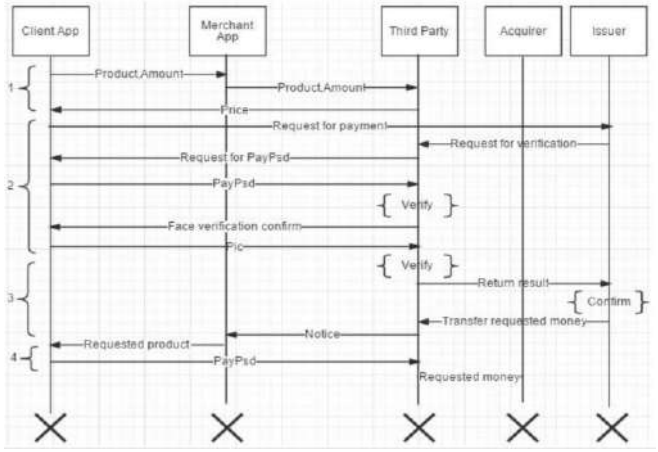

Fig. 4. Mobile Payment Security Processes and Interfaces Design

1) Find what you need and confirm the order with the dealer. Once the merchant receives the customer's request, they must send the request to a third-party regulatory agency, which includes the product name, unit price, amount, etc. The total price is sent after your third party certificate.

2) You need to provide a PayPal password after the customer has received and confirmed the total price. When a third party confirms the payment password, a request is sent to an external image to the client.

3) Once verification of identity and password has been completed, the issuing institution transfers the amount necessary for the transaction to the third-party account. He then sends the seller a notice of receipt to inform the customer of the third-party vendor that the goods will be delivered.

4) The customer needs to confirm it to the third party that receives the goods online. After that, the amount of payment necessary to the third party is transferred to the acquirer. At this point, the deal is over.

In this case, four request APIs are displayed in Table III to facilitate access to their mobile phone applications and identity technology.

TABLE III
NECESSARY FOR THE FACE AUTHENTICATION

API Name	Function Description
Face Detection API	Detect human face in images, then the detected face will be marked
PCA Processing API	Do 2DPCA to existing data
Face Matching API	Compare two processed face images
Grayscale Conversion API	Put color image convert into gray images

VIII. SECURING MOBILE BANKING ON ANDROID WITH SSL CERTIFICATE PINNING

Let's say you want to exchange some sensitive data between your application and a server. SSL should do the trick, but in many cases, you'll have to send sensitive data between your application and server. Take mobile banking applications for example. The last thing you want is a malicious hacker to steal someone's bank account info – or worse, their money [18].

Security is crucial for a mobile banking solution, so you'll be using SSL to keep that data safe and secret. But there's a catch. The app has no relationship with the trust store of the device to enforce security using static SSL certificates. It's not easy to destroy fixed-coded stores in your app. The app must be compiled, edited, and reassembled, and cannot sign the same Android activation key used by the original developer of the app. Table IV shows the present Uzbekistan mobile banking implementation solutions.

TABLE IV
UZBEKISTAN MOBILE BANKING IMPLEMENTATIONS SOLUTIONS

IX. MOBILE BANKING ANALYSIS

Central Bank of Uzbekistan Tashkent, [17] on 1 April 2013

	WAP	SMS &USSD	SMS &WIG
Transmission Speed	The transfer rate of any mobile banking solution depends on several factors. This depends on the signal strength received by the user's mobile phone. Thus, this depends on the user's location, network traffic, the number of base station towers around the user's mobile device, etc. All these factors affect the transfer rate and you cannot do real experiments.		
Cost for Bank Server	GPRS is generally cheaper than SMS.	One SMS message for reply	Multiple SMS reply messages required.
Usability	Mobile phone WAP browser interface.	It requires no menu. The user interface depends on how the users interact with their mobile phones to send SMS messages.	Menu-based user interface.
Compatibility	Requires mobile phone to be WAP capable and GPRS, EDGE or 3G enabled.	Any mobile phone that can support USSD and SMS can use this service.	Requires mobile phone to be SIM Application Toolkit (SAT) compatible. It is SIM card dependent.
Security	Standard WTLS protocol. No End to End encryption.	USSD String sent in plaintext. Authentication relies on IMEI.	USSD string and SMS message transmitted in plaintext.
Cost for Customer	It depends on the amount of data required to be sent.	USSD is for free. One SMS message required	Multiple SMS messages required.

the number of users of distance banking services in Uzbekistan made up over 149,000, the central bank noted that the number of SMS-banking and mobile banking services made up 106,925 units and internet banking 42,098 units as of 1 April 2013.

Compared to 1 January 2013, the number of users of SMS banking and mobile banking service rose by 37,600 and internet banking – by 2,930 units Fig. 5.

Fig. 5. Number of users of distance banking services

According to the central bank, the National Bank of Uzbekistan (34,300 users), Ipoteka Bank (30,314 units) and Microcreditbank (15,477 units) are leading on a number of users of distance banking services as showing in the Fig. 6 and Table V.

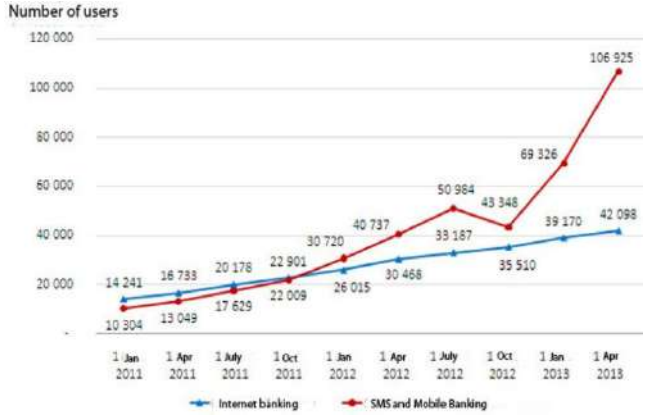

Fig. 6. Number of users of distance banking services by type of system

TABLE V
MOBILE BANKING SERVICES OFFERED BY SOME OF THE BANKS IN UZBEKISTAN

No	Name of the Bank	Internet banking Users	SMS-banking and mobile banking users	Total
1	National Bank of Uzbekistan	4227	30071	34298
2	Uzpromstroybank	2042	1348	3390
3	Agrobank	1765	749	2514
4	Ipoteka-Bank	3158	27255	30413
5	Microcreditbank	2385	13062	15447
6	People's Bank	1204	-	1204
7	Savdogarbank	459	-	459
8	Qishloq Qurilish Bank	1239	8692	9931
9	Turon Bank	981	613	1594
10	Hamkor Bank	4147	4767	8914
11	Asaka Bank	1503	8513	10106
12	Ipak Yoli Bank	3229	2042	5271
13	Uzbek-Turkish Bank	177	128	305
14	Trust Bank	1352	970	2322
15	Aloqabank	1226	1789	3015
16	KDB Bank Uzbekistan	217	498	715
17	Turkiston bank	227	25	252
18	Sederat Iran	11	12	236
19	Samarkand Bank	6302	429	6731
20	Universalbank	258	425	683
21	Kapitalbank	2803	3907	6710
22	Ravnaq Bank	64	33	97
23	Davr-Bank	704	-	704
24	Credit Standard Bank	34	215	249
25	Invest Finance Bank	1028	431	1459
26	Amirbank	52	38	90
27	Asia Alliance Bank	610	329	939
28	Hi-Tech Bank	298	82	380
29	Orien Finans Bank	396	502	898
	TOTAL	**42098**	**106925**	**149023**

Fig. 7 shows [19], [20], the number of ATMs and information terminals for 100,000 adults have so fast grown; the development of non-cash bank payment system was not silky. However, the growth rate of bank cards on an annual basis is much faster than the initial increase in ATM cards.

In general, Uzbekistan's prudent and cautious approach seems to have achieved its goal. It helps to avoid the double crises faced by most economies in transition, thereby protecting social stability and reducing the negative impact of structural reforms on employment and economic growth. The change in state ownership, the introduction of credit bureaux and mortgage registration, and the rapid development of non-cash payment methods show that the banking industry is gradually being integrated into market-based systems.

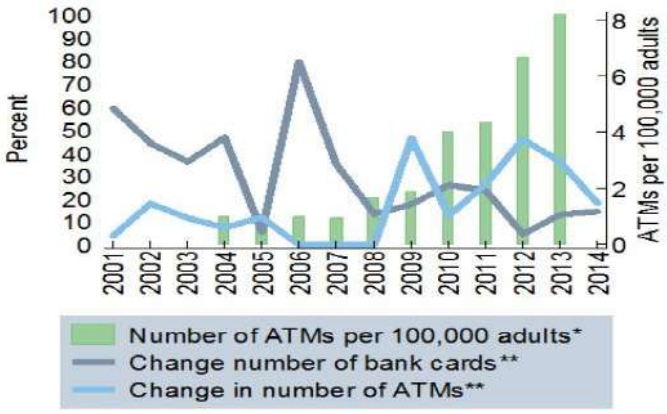

Fig. 7. Bank Cards and ATMs

X. CONCLUSION

For today, online banking is one of the modern tools, which allow banks to increase their profitability and increase their profitability client base. This article examines the world-wide issues and challenges online banking as well as an overview of the current state of online banking in Uzbekistan. The Uzbek banking system remains under State control through a series of regulatory measures, legislation, declarations and complex practices. Most bank assets are still in state-owned or state-controlled banks, and most of the loans are directed by the government or directed to develop a pre-determined industrial sector. By limiting the role of banks as a financial intermediary to reform the slow financial system, it limits the ability of citizens and private companies to access credit and other financial services

This work is to classify and analyze the Security issues and challenges in Mobile banking in Uzbekistan. The majority of the customers in Uzbekistan are using online banking or ATM. However, around 40 % of customers are using mobile banking where the remaining people 60% are not using this technology.

ACKNOWLEDGMENT

This work was supported by the Institute for Information and Communications Technology Promotion (IITP) grant funded by the Korea government (MSIT) (No.2018-0-00245), And it was also supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science, and Technology (grant number: NRF2016R1D1A1B01011908).

REFERENCES

[1] Customer adoption of banking technology: the case of uzbekistan . *International Journal of Bank Marketing* vol.pp.15-25

[2] A. D. Bank, "Technical assistance to the Republic of Uzbekistan for Development of the capital market Uzbekistan, Manila: *ADB*, 2017.

[3] A.V. Akimov, and B. Dollery. "Uzbekistan's Financial System. An Evaluation of Twelve Years of Transition." *Problems of Economic Transition* 48, no. 12, pp. 6–31, 2017

[4] K.D. Ghosh, S.C Ruziev. "Analysis of Mobile banking Economic Performance in Uzbekistan" vol 26.no.1, pp. 7-30

[5] https://m.hamkorbank.uz/en.The History of the Banks in Uzbekistan

[6] I.A.BOQIYEV, "Research on Security Payment Technology Based on Mobile Phones" , pp. 1-4, 2017

[7] Click system in Uzbekistan in 2011-2018. Annual report of central bank in Uzbekistan . https://click.uz/, http://www.gov.uz/government/cbu/cbu_0.htm

[8] A.V.Vahobov "Public key infrastructure for mobile banking security" vol 66.no.2, pp 12-20, 2015

[9]. J. Nie and X. Hu. "Mobile Banking Information Security and Protection Methods", *International Conference of Computer Science and Software Engineering*, , pp. 587-590, 2008.

[10] C. Narendiran, S. Albert Rabara, and N. Rajendran. Public key infrastructure for mobile banking security, *Global Mobile Congress*, pp. 1-6,2009.

[11] I. Brown, Z. Cajee, D. Davies, and S. Stroebel, "Cell phone banking: predictors of adoption in South Africa--an exploratory study, *International Journal of Information Management*,Vol.23, pp. 381-394, Oct.2003.

[12] D. Y. Liou, "Four - scenario analysis for mobile banking development contextualized to Taiwan", *Management of Engineering & Technology, PICMET*, pp. 2634-2642, 2008.

[13]. H. Wu, A. Burt, and R. Thurimella. Making secure TCP connections resistant to server failures, *Computer Security Applications Conference*, Proceedings. 19th Annual, pp. 197-206,2003.

[14]. H. Harb, H. Farahat, and M. Ezz. SecureSMSPay "Secure SMS Mobile Payment model", *Anti - counterfeiting, Security and Identification ASID*, pp. 11- 17,2008.

[15] T. Wilson, ― Malicious mobile ode, ‖ Internet Business, pp. 52-3, Feb.1999.

[16] T. Holz, M.Engelberth, F. Freiling," Learning More about the Underground Economy", *ESORICS*, LNCS 5789, pp. 1–18, 2009

[17] Tashkent, Uzbekistan, April, 2013 "Over 149,000 users use distance banking services " https://www.uzdaily.com/articles-id-22798.htm

[18] I. Kušt., "Securing mobile banking on Android with SSL certificate pinning" March 12th, 2014 https://infinum.co/the-capsized-eight/securing-mobile-banking-on-android-with-ssl-certificate-pinning

[19] M.Ahunov.,"Uzbek banking system: some history and current state" July 26,2015, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2636002

[20] A. Abdullaev, M. A. Al-Absi, A. A. Al-absi, M. Sain, H. J. Lee" Security Challenge and Issue of Mobile Banking in Republic of Uzbekistan: A State of Art Survey" *International Conference on Advanced Communications Technology (ICACT)* February 17 ~ 20, 2019

[21] Uzbekistan-bankingsystems https://www.export.gov/article?id=Uzbekistan-Banking-Systems/ 2019

AZamjon Abdullaev was born in Uzbekistan 1992, received his BS degree in finance from Tashkent financial Institute in Uzbekistan 2011-2015. Currently, he is a Master candidate student in the Department of Computer Engineering at Dongseo University, Korea. His research interests include Mobile Banking, Wireless Sensor Networks, Cryptography, and Network Security.

Mohammed Abdulhakim Alabsi was born in Yemen 1987, received his BS in Computer Application from Bangalore University in India. He earned his (MS) degree at Dongseo University, South Korea in 2018. Currently, he is a PhD. student in the Department of Information and Communication Engineering at Dongseo University, South Korea. His research interests include IoT, VANET, UAV, artificial intelligence, cryptology, network security, computer networks and digital communications.

Ahmed Abdulhakim Al-Absi was born in Yemen 1984, he is an Assistant Professor and Head of Smart Computing Department at Kyungdong University – Global Campus in South Korea. He earned his PhD in Ubiquitous Computing at Dongseo University, South Korea in 2016. His research interests include database systems, big data, hadoop, cloud computing, distributed systems, parallel computing, high-performance computing, VANET, and bioinformatics. He received a Master of Science (MS) degree in Information Technology at University Utara Malaysia, Malaysia in 2011 and a Bachelor of Science (BS) degree in Computer Applications at Bangalore University, India in 2008.

Mangal Sain was born in India 1979, received the M.Sc. degree in computer application from India in 2003 and the Ph.D. degree in computer science in 2011. Since 2012, he has been an Assistant Professor with the Department of Computer Engineering, Dongseo University, South Korea. His research interest includes wireless sensor network, cloud computing, Internet of Things, embedded systems, and middleware. He has authored over 50 international publications including journals and international conferences. He is a member of TIIS and a TPC member of more than ten international conferences.

HoonJae Lee was born in Korea 1962, received his BS, MS, and Ph.D. degrees in electronic engineering from Kyungpook National University, Daegu, Rep. of Korea, in 1985, 1987, and 1998, respectively. He is currently a professor in the Department of Information Communication Engineering at Dongseo University. His current research interests include Password Theory, Network Security, Side-Channel Attack, and Information Communication/Information Network.