International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-7 Issue-5, January 2019

A Novel Cryptographic Data Security Approach for Banking Industry to Adopt Cloud Computing

Kanika Tyagi, Anuranjan Mishra, Mayank Singh

Abstract: ***As the advancement in technology ,banking industry is facing several changes. Customer is now at the driving seat of new financial industry scenario as the whole control is now in the hands of customer. Due to the prospering technology, traditional banking has totally changed. Banks need to establish a new customer driven environment with innovation in business models .Being a most trending technology many organizations wants to adopt clouds as a cost effective strategy ,to provide innovative client services and to increase and manage IT efficiency .But banking industry still have some issues such as security ,privacy ,compliance and authenticity which somewhere produces an obstacle to adopt this flexible and agile technology. So there is a need for some mechanism which can provide a secured cloud environment in banking industry. This paper presents a mechanism to secure the cloud in banking industry by combining some algorithms viz; Password Based Key Derivation Function (PBKDF2),Argon2, AES-256 and IDA algorithm. This paper also shows features of clouds and security challenges of clouds in banking industry.***

Keywords: ***PBKDF2, Argon2,AES(Advanced Encryption Standard),IDA(Information Dispersal algorithm)***

I. INTRODUCTION

Cloud computing basically strike the idea of storing and managing data on virtualized servers so that customer and organization can access the data all over the world from anywhere at anytime. But banks cannot afford the risk of security breach since security of personal and financial data is topmost priority for banks .Therefore to move banks into cloud computing environment it is essential that security issues should be considered first. There are some features of adopting cloud in the banking industry:

Reduce expenses: Adoption of cloud in banking industry lead to a cost effective method. While a bank uses a cloud computing, there is no need to invest a large amount in new hardware and software[1]..

Revised Manuscript Received on 30 January 2019.
***** Correspondence Author
Kanika Tyagi*, Research Scholar, Noida Internatiinal University.
Dr. Anuranjan Mishra, Professor and Director, Accurate Institute of Management & Technology, Greater Noida.
Dr. Mayank Singh, Professor and Head, Department of Computer Science and Engineering, Krishna Engineering College, Ghaziabad.

Beside that as we know that in cloud qe uses pay per used technique which enables to pay only for the needed resources[2]. **Improves flexibility and scalability:** Cloud enables banking industry to respond as per the user's demand [3]. Technology can be scale up and scale down as per the changing market scenario

Business Regulation: If a bank uses cloud, there are less chances of data loss due to fire, disaster and theft [2]. Cloud computing provides a high degree of data backup and recovery.

Improves client relationship: Having unlimited computing powers, cloud build strong relationship with customers. Transaction banking enables buyers and sellers share a same plateform so that the payment process becomes more efficient. [3]

But when a bank moves into cloud environment it faces many challenges.

Security: While banks keep their data over cloud then security of commercial and personal data is at stake. Banks cannot allow the risk of security breaches [4].

Data segregation: As we know that data on clouds is stored globally dispersed environment so there are many chances for data loss which cause an obstacle [6] to adopt this prospering technology.

Data location: When customers use cloud technology they have no idea about data location [6] . Dispersed location of data lead to lack of control on data and it is very risky for customers.

Regulatory Compliance: Customers are basically liable for the security of their data even when traditional service providers most lean towards external audits and security certificates [5] . Certain compliance arrangement want that data should not be mixed with other data on shred servers.

Trust: There should be trust between human to machine, Human to human and machine to human [7]. If a user places his crucial data on cloud then it is only because of trust.

Data Recovery: It means the process of attaining the data that has been lost, corrupted or accident [6].

Privacy and Confidentiality of data: It refers to the trait that data is not accessible to the unauthorized user [7]. In other words only authorized user can access the data and use any sensitive data and can take any information out of that data.

Data integrity: It means that our data on cloud does not contain any tempering and alteration[7].

II. TRADITIONAL HASHING VS KEY DERIVATION FUNCTION

While security is concerned in the banks, then password is the crucial and most important aspect. Passwords are mostly used to protect secret data as in banks. Password scheme is used for authentication So in this way we can say that password should be as strong as it can create a strong wall against various intruders attack like brute force attack and dictionary attacks [8].

When user chooses a password they keep that simple and easy to memorize which can be recalled at the time of login and also sometimes user uses same password for various services like banking, online shopping and social networking sites[8]. In this way user opens gateway to put their data as a serving for hackers. The password chosen by user has low entropy and randomness [9]s so they cannot be used directly as a cryptographic key. So a strong mechanism is needed here to secure the password which automatically leads to secured cloud environment.

A key derivation function is one of the best solutions to secure the password. In key derivation function user chosen password is used as an input to generate one or more cryptographic keys. These cryptographic keys are applied by encryption and decryption [10].

Having low entropy and randomness [9] of user generated secrets are susceptible to attacks. By using exhaustive search methods attackers discover the actual passwords and get access the account

Similarly when uses graphical passwords it also have low entropy and they are also not full proof arrangements against intruders attacks and they provide 4-5 bytes of security on average.

Then a technique called “Key stretching “ [8] provides security against such attacks. Cryptographic hash functions take large amount of data and produces fixed amount of output which is called hash. One cannot get original message with this hash value and two messages cannot have same hash value [8]. Normally user chooses some passwords and they are stored in database then it acts as a password. But there is problem too. If many users are having the same password, the hash result will be same too .and if one of these password is revealed then other users will also loss their credentials. similarly if one user uses same password for various services like social networking sites or banking ,disclosure of one of these accounts somewhere put a question mark for the security of other involving services .Thus we have a technique called “salt” perimeter. Salt is a small value, usually consisting of 8 random bytes. While a user creates new account a random salt is generated which is appended with the passphrase during hashing [8] . The same password produces different hashes for different accounts and thus the problem of simple hashed password that is generated by same passphrase is prevented. At the authentication phase, passing of salt and password is done during login procedure and result is compared with the stored password hash value to validate [10] the user.

III. BACKGROUND WORK

A. Manisha R Shinde and Rahul D. Taur [2] proposed algorithm for data security and privacy in cloud storage .They discussed about the cloud, its models and cloud security. They also proposed an encryption algorithm by integrating substitution cipher and transportation cipher. But this approach was not free from brute force attacks.

B. Dr. Sheel Ghule, Rupali Chikhale, Kalpesh parmar [3] explained the cloud computing in banking services. They shown deployment model of cloud in banking .They also shown the good and bad side of using clouds in banks.

C. Garima Saini and Naveen Sharma [11] stated that cloud comprises of many servers and it follows client server architecture. So to protect the cloud he suggested a mechanism in which he presented the blend of two algorithms i.e. Digital Signature Algorithm (DSA) and Data Encryption Standard(DES) with staganography to enhance the security. But it was observed that its time complexity was high

D. Levent Ertaul, Manpreet kaur,Venkata Arun Kumar R Gudise [8] implemented the performance of PBKDF2, Bcrypt Scrypt algorithms. In this paper it is concluded that PBKDF2 is employing many applications and it was considered the best password manager. PBKdF2 is fast while Bcrypt is slow and Bcrypt and Scrypt also are memory hard functions which takes large resources and computational power to crack.

E. Alex Biryukov, Daniel Dinu and Dmitry Khovratovich [12] shown the password hashing scheme in their research. They thrown light on various problems of existing schemes They offered an solution called Argon2 in design of memory hard functions. They recommended the Argon2 for the high performance applications. They discussed the inputs,operation and indexing of Argon2 . Beside that they also illustrated the features of Argon2 such as high performance, parallelism, design rationality, scalability and so many.

F. Y.D Vybornova[13] used password based key derivation function as one of the blum-slum –shub pseudo-random generator applications. They proposed the algorithm to derive cryptographic key from easy to remember password., which somewhere makes very difficult to implement dictionary attacks and brute force attacks.

G. Jean Raphael Ngnie Sighom, Pin Zhang and Lin You [14] proposed a enhancement for data migcration in cloud. They used the AES (Advanced encryption standard -256), IDA(Information Dispersal algorithm) and SHA-512 (Secure Hashing algorithm) to secure the clouds. This blend provided a secured and fast execution time for medium thresholds.

H. Dr. K. Subramanian, F. Leo John[15] shown data slicing in multi cloud storage to secure the cloud. They presented a framework in adoption of multi cloud storage service.

But this method was not able to resolve other security issues as non repudiation .

I. Amanjot Kaur, Manisha Bhardwaj[16] proposed hybrid encryption for cloud database security using 3DES, Randon Numner generator and RSA. But this scheme creates overhead on the query performance as it has multilevel encryption and decryption and when the size of data is increased its computation time is also increased .

IV. PROPOSED WORK

As today mostly organizations wants to put their data on cloud storage so as the banks. But security and user privacy are some prominent issues which cannot be ignored. So main aim of this propose work is to secure the cloud over banking industry so that banks can adopt this agile technology without hesitation.

The proposed work comprises of 3 basic steps:

- Key generation using blend of PBKDF2 and Argon2
- Encryption and data Slicing using AES-256(Advanced Encryption Standard) and IDA(information Dispersal Algorithm)
- Data Assembling and decryption using IDA and reverse of AES algorithm

The block diagram of proposed work is as follows:

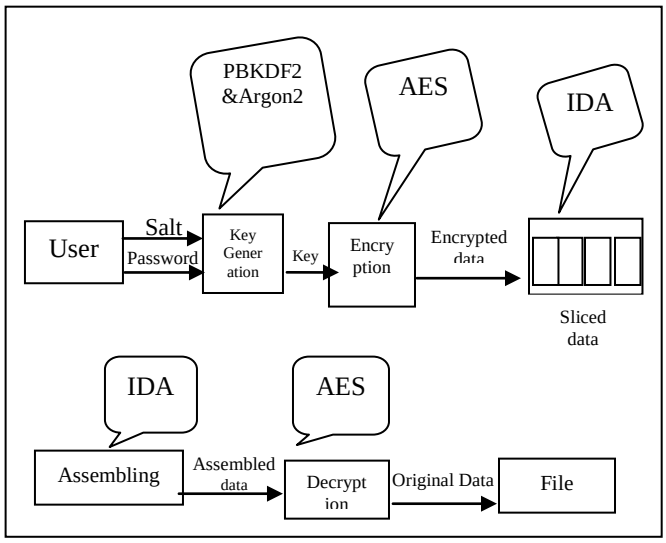

Fig:1 Block diagram of proposed work

Password Based Key Derivation Function2 (PBKDF2):

PBKDF2 is recommended by NIST (National Institute of Standard & Technology) to derivate the key.PBKDF2 is an algorithm to produce cryptographic key of some length from some secret value or easy to remember password [8]. This key is used to protect the data or to recover the data, for verification and for data authentication as well as to generate digital signatures.

PBKDF2 uses pseudorandom functions PRF. These are commonly implemented by HMAC. As a hash algorithm it uses SHA-256/512[17]. PBKDF2 takes the following parameters as input:

- A user chosen password (p)
- A random salt (s)
- An iteration count (c)
- Secret key length(s_key length)

It generates the secret key s_key as the following way:

s_key= PBKDF2 (PRF, p, s ,c, s_key len)

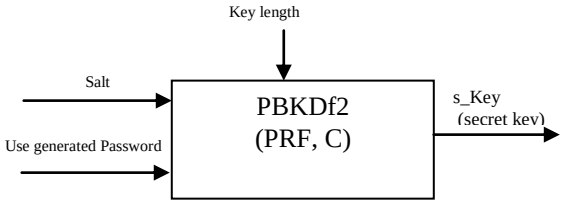

Fig:2 Working of PBKDF2

PBKDF2 applies pseudorandom functions to the input password along with a salt value and repeats the process many times to produce a derived key which can then be used in the operations like encryption/decryption [9] . The password cracking becomes more difficult by introducing the extra computational work (key stretching).Adding salt to the password decrease the threats to precomputed hashes. As more rounds lead to harder an attack. As per the standard written in 2000 count iterations was 1000 but as of today most software uses less than 5000 rounds[18].

The main aim of dictionary attacks is to gain access by trying familiar passwords which are stored in special treated dictionaries. There are also chances of brute force attacks in which attackers tries all combination off characters[8].

The main idea of using PBKDF2 is that it slow down the dictionary attacks and brute force attacks by increasing the time needed for each attempt of the attacker to find the correct password[9]. Except that use of salt value makes it impractible to precompute the hash values and to implement table attacks.

Algorithm: The key derivation function accepts the following input parameters:

s_key= PBKDF2 (PRF, p, s ,c, s_keylen)

Where PRF is a pseudorandom function,

p is the user generated password from which key is generated

s is a cryptographic salt

c is the no. of counts/iterations to hash the password

s_key is the derived cryptographic key

s_keylen is the desired length of secret key

Each block B_i of secret key s_key is computed as follows:

s-key
$=B_1\|B_2\|.....\|B_{s\_keylen/hlen}$

The function f is the Xor (^) of c which iteration of iterated PRFs.

F (p, s, c) =Y_1^Y_2^……. ^Y_C

Where:

Y1= PRF (p, s‖INT_32_BE)

Y_2=PRF (p, Y1)

Yc=PRF (p, Yc_{-1})

In this way PBKDF2 makes harder for intruder to guess the original password.

Argon2: Argon2 is the winner of Password hashing Competition (PHC 2015) Argon 2 has two variants: Argon2d and Argon2i [12].

Argon2d is based on data –dependent memory access and it is designed to hold up against brute force attack.Argon2i is based on data independent memory access [18] and it is basically for password hashing and password based key derivation functions. Argon2i is having more passes so it is slower. We have two types of inputs in Argon2: Primary inputs and secondar98 to y inputs.

Primary Inputs contain password (p) of length (0 to 2^{32}-1 bytes) and salt(s) from (8 to 2^{32}-1)[12]

Secondary Inputs comprises degree of parallelism p, tag length, memory size , number of counts and associated data X. Argon2 uses Blake2b as hash function and BlaMka as the compression function.

Initially it takes inputs password (p) and salt(s) which are hashed along with other parameters. In this, memory is organized as 2-d array and is represented by B[12]. The memory comprises of compression function for which indexing function is used as input. For the variant Argon2i,indexing is password and salt independent and for variant 2d,indexing is password dependent. There is also a hybrid variant called Argin2di. It is a mixture of two approaches Argon2d and Argon2i .In this some of the indexing is performed by data independent functions and the remaining being performed by data dependent functions. This process repeats for variable number of passes and after the final iteration the memory element of the last column are XORed. To obtain the final outcome result is hashed[18].

IDA (Information Dispersal Algorithm)

An IDA is the process of slicing a file and data packets into pieces so that they unrecognizable as they placed in storage arrays at dispersed location in network [14] [15]. This sliced data can be reassemble at receiving end using the appropriate key.

First considered by rabin [19] ,in this algorithm the file F of length L is split into m pieces F_i , so that knowledge of any n pieces help to reconstruct the file F.

V. WORKING OF PROPOSED ALGORITHM

Our proposed approach consists of password based key generation using blend of PBKDF2 and Argon2 to generate the most secured key, AES-256(Advanced Encryption Standard) foe encryption and decryption and IDA(Information Dispersal algorithm) to slice the data to store it on various dispersed locations. Steps for the given approach are as follows:

Step:1 Key generation

This step is a blend of two algorithms i.e. PBKDF2 and Argon2. In this user generated password and salt will be accepted as input to the PBKDF2. After applying required no. of iterations and defining the length of the key a secret key will be generated. This secret key will work as a password for next phase of this step. In this phase Argon2 takes two inputs salt and password (generated secret key in first phase). Now there are some specified rounds of Argon2 and a most secured key C_key will be generated which will be used in the encryption phase as a cryptographic key.

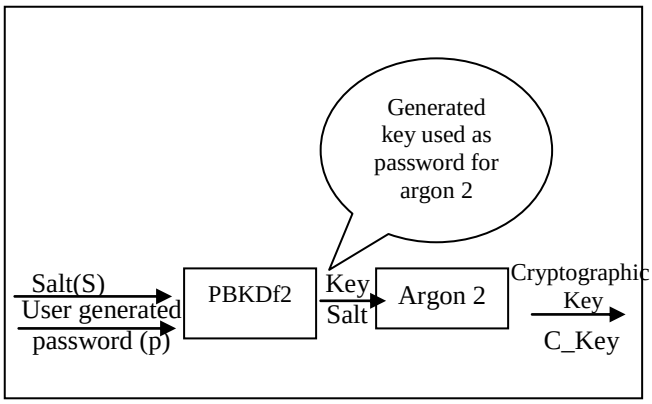

Fig:3 Key generation

Step:2 Encryption and Data slicing

This step has two security levels :encryption with AES-256 and data slicing using IDA algorithm.

During this process user's original data or file E is firstly encrypted using AES-256 algorithm. The cryptographic key c_key generated in first step will be used here. After the encryption, the encrypted file E' is broken into m separated files at dispersed locations. These files are located on various locations in such a way that if a user has knowledge of atleast n of these m slices then it can be used to reassemble the encrypted file E'=ς(E,c_key)

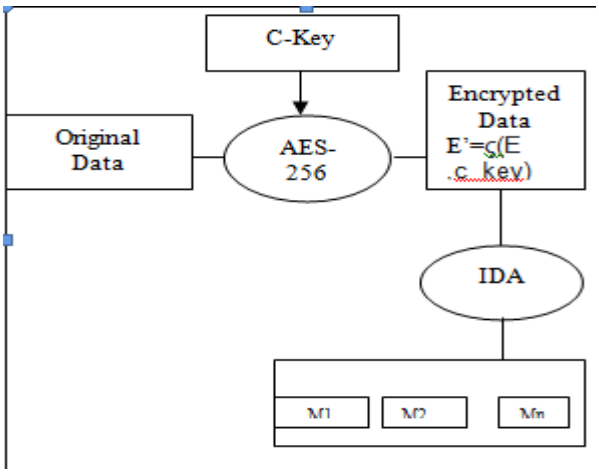

Fig:4 Encryption and data slicing

Step:3 Reassembling and decryption:

In this step IDA algorithm will be applied to the resulting slices as shown in figure:

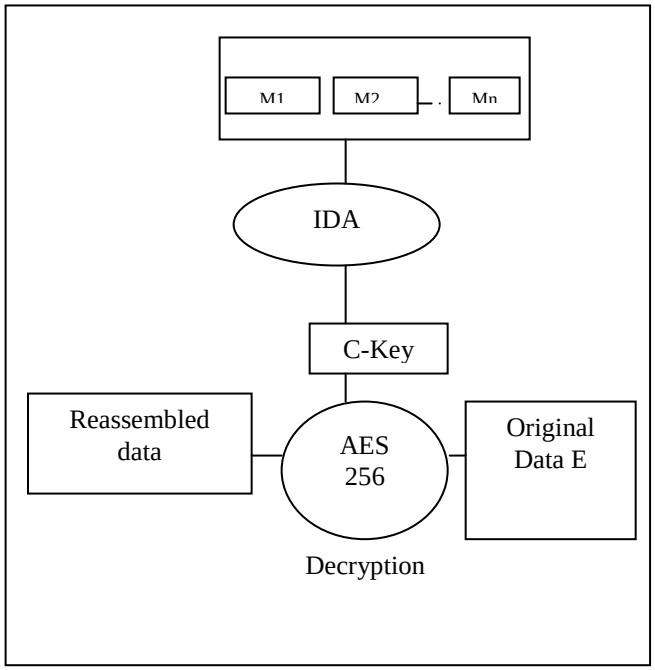

Fig:5 Reassembling and Decryption

We apply IDA algorithm to reassemble the encrypted file E' and then recovert the original file E having the cryptographic key c_key with AES-256.Now compute the decrypted version of E using AES-256 as using E=Δ(E',c_key).

VI. CONCLUSION AND FUTURE SCOPE

In the proposed algorithm some drawbacks of existing algorithms are removed. As we know that data on cloud is in the form of multi tenant environment where data and resources are shared. So to adopt cloud technology in banking industry it should be ensured whether the data is secured or not. In our proposed system we presented the combination of PBKDF2,Argon2, AES-256 and IDA algorithm. PBKDF2 and Argon2 are key derivation function used for key generation which provide verification and authentication. AES-256 for data confidentiality and IDA to break the encrypted data . PBKDF2 help user to lesser the attacks and at the same time argon2 eliminate all the weaknesses of pbkdf2 and makes the password hacking next to impossible. As secured password lead the secured data so our approach secured the password .Our proposal achieve higher degree of security and also better performance .

.

REFERENCES

1. Stud. Ranjana Singh, AS. Prof Kirti Patil, AS. Prof Ashish Tiwari, "A survey on online banking authentication and data security", International Journal of Advanced Research in computer Engineering and Technology, Volume 5,Issue 2,2016.
2. Manisha R. shinde & Rahul D. Taur,"Encryption Algorithm for data security and privacy in cloud storage", American Journal of Computer Science and Engineering Survey, Original article ,ISSN 2349-7238.
3. Dr. Sheel Ghule, Rupali Chikhale, kalpesh Kumar," Cloud Computing in Banking Services", International Journal of Scientific & Research Publications, Volume 4, Issue 6 ISSN 2250-3153, 2014.
4. P.S.V. Sainadh,U. Satish Kumar, S. Haritha Reddy, " security issues in Cloud Computing", International Journal of Modern Trends in Science and Technology", Volume 3,special issue no.:01, ISSN: 2455-3778, 2017.
5. Dinesh Taneja, SS Tyagi, "Information Security in Cloud Computing: A systematic Literature review and Analysis", International Journal of Scientific Engineering and Technology", Volume 6,Issue 1,ISSN: 2277-1581,2017.
6. Chitrali Agre," Implementation of Cloud in Banking sector", International Journal of Computer science and Information Technology research, Volume 3, Issue 2 ,ISSN: 2348-1196, 2015.
7. Akshat Ajabrao Uike, Dr. M.A.Pund, " An Overview of Cloud Computing: Platforms, security Issues and Applications", International Journal of Science Technology Management and research", Volume 2, Issue 5, ISSN : 2456-0006,2017.
8. Levent Ertaul, Manpreet Kaur,Venkata arun Kumar R Gudise, " Implementation and performance analysis of PBKDF2, Bcrypt, Scrypt Algorithms", International conference Wireless Networks, ISSBN : 1-60132-440-5.
9. Andrea Visconti, Simone Bossi, Hany Ragab, Alexandro Calo, " On the weaknesses of PBKDF2",International Conference on Cryptography and Network security", Springer International Publishing, LNCS 9476.
10. George Hatzivasilis," Password –Hashing Status", Journal Cryptography 1020010.
11. Saini ,Garima, Naveen Sharma, " Triple Security of Data in Cloud Computing", International Journal of Computer Sience & Information Technologies, 5.4,2014
12. Alex Biryokov, Daniel Dinu, Dmitry Khovratovich," Argon2: the memory hard function for password hashing and other applications," version 1.3 of Argon2:PHC release,2017.
13. Y. D. Vybornova," Password –based key devivation function as one of Blum-Blum-Shub Pseudo-random generator applications",3rd International Conference," Information Technology and nanotechnology, published by Elsevier, ITNT 2017,ISSN: 1877-7058
14. Jean Raphael Ngnie Sighom,Pin Zhang and Lin you, "Security Enhancement for Data Migration in the cloud", Future internet,2017.
15. Dr. K. Subramanian, F.Leo.john," Dynamic Data Slicing in Multi Cloud Storage using Cryptographic Technique", World congress on computing and communication Technologies, 978-1-5090-5573/17/IEEE
16. Amanjot Kaur, Manisha Bhardwaj, "Hybrid Encryption For Cloud Database Security" ,International Journal of engineering Science and Advanced Technology", Volume 2, Issue 3, ISSN : 2250-3676,2012.
17. VPN Tracker, Company Connect," Connection Safe security Architecture," equinox
18. Turan,MS,E.Barker,W.E.Burr and L.Chen ," Recommendation for password based key Derivation",http://csrc.nist.gov/publications/nistpubs/800-132/nist-sp800-132.pdf
19. Rabin, M.O. Efficient dispersal of Information for security, Load balancing and fault tolerance J. ACM,1989,36,335-348

AUTHORS PROFILE

Kanika Tyagi is a research scholar at Noida Internatiinal university. She has completed her Masters in Computer applications in 2013.She has published Many papers in various journals.

Dr. Anuranjan Mishra is professor and Director , Accurate Institute of Management & Technology, Greater Noida. Prof. Misra is a Senior Member of CSI, IACSIT, IACNG, IRACST, SDIWC and member of CSTA, ISOC, ICE, AEE, IFETS, ISMCDM, SIGSE.
.

Dr. Mayank Singh is currently working as a Professor and Head, Department of Computer Science and Engineering at Krishna Engineering College, Ghaziabad**.** He has 12+ years of extensive experience in IT industry and Academics in India. He has completed his Ph.D. in Computer Science and Engineering from Uttarakhand Technical University in 2011