Secured Network Coding approach for Cloud Storage

Preethi Jothsna[1], A Ramesh[2]
[1]M.*Tech (CSE)., Dept of CSE, Nova College of Engineering And Technology Jupudi village and ibrahimpatnam*
[2]*Assistant Professor, Dept of CSE, Nova College of Engineering And Technology Jupudi village and ibrahimpatnam*

***Abstract*— This paper focuses the ingrained relationship between secure cloud storage and secure network coding. The secure cloud storage protocol is that the user can check the data integrity without possessing the actual data. The secure network coding uses the concept of data fragmentation. Though different and studied independently they can work together to give effective results. It shows systematic construction of secure cloud storage protocol when secure network coding protocol is used with it. Further two specific secure cloud storage protocols based on two recent secure network coding protocols are proposed. First is security mediated anonymous cloud storage is proposed and second is third party auditable secure cloud storage. It will give us the effective and efficient mechanism for secure cloud storage.**

I.INTRODUCTION

Cloud Facilities expansion of green computing technologies, embedded devices integrated with wireless technologies such as storage, platform and various other technologies such as Remote Clouds. Besides usual personal computers, billions of small, tiny devices will be connected to what is called Future Internet [1] With the rapid development of network bandwidth, the Volume of user's data is rising geometrically. User's requirement cannot be satisfied by the capacity of local machine any more. Therefore, people try to find new methods to store their data. For more powerful storage capacity, a growing number of users select cloud storage. Cloud storage is a cloud computing system which provides data storage and management service. With a cluster of applications, network technology and distributed file system technology, cloud storage makes a large number of different storage devices work together coordinately.

Nowadays there are lot of companies providing a variety of cloud storage services, such as Dropbox, Google Drive, iCloud, Baidu Cloud, etc. These companies provide large capacity of storage and various services related to other popular applications. However, cloud storage service still exists a lot of security problems. The privacy problem is particularly significant among those security issues. In history, there were some famous cloud storage privacy leakage events. User uploads data to the cloud server directly. Subsequently, the Cloud Server Provider (CSP) will take place of user to manage the data. In consequence, user do not actually control the physical storage of their data, which results in the separation of ownership and management of data.

Figure 1.1: Architecture of Cloud Computing

II. INTRODUCTION TO AUDITING SCHEME

Cloud computing is a new computing mode that was created after peer-to-peer computing, grid computing, and utility computing and distributed computing. The core concept of cloud computing is resource renting, application hosting and service outsourcing. Through

virtualization technology, it forms distributed computing nodes into a shared virtualization pool in order to provide services for users. With cloud computing technology, users and enterprises do not need to spend much on the acquisition and maintenance of hardware in their early stages. In addition, powerful computing and storage capabilities also make users more willing to rely on the cloud to handle a variety of complex tasks. When users choose to deploy a large number of applications and data to the cloud computing platform, the cloud computing system accordingly becomes the cloud storage system. Cloud storage systems give users mass storage capacity at a relatively low price, and provide a platform for sharing data between users (data sharing means that a user in a group uploads data to the cloud, and the rest of the group The associate editor coordinating the review of this manuscript and approving it for publication was Songwen Pei. can
access/modify the data). However, highly centralized computing resources means cloud storage faces severe security challenges. A malicious cloud server is able to discard all the shared data and generate a valid proof of data possession by reserving some intermediate results or a previous valid proof, which we refer to as a replace attack and a replay attack, respectively. A malicious group member is able to modify other member's data in that group without being discovered. A malicious agent is able to collude with illegal group members to steal user data and identity information. As far as we know, the three points mentioned above are still open challenges to design a secure integrity auditing scheme for shared data with Secure Network Coding Techniques computing on the client side. To solve those challenging problems, we proposed a Secure Network Coding Techniques secure auditing scheme for shared data in cloud storage (LSSA). Similar to the cloud storage audit scheme, using the Third Party Medium (TPM) instead of group members to calculate the authentication label and audit data integrity results in Secure Network Coding Techniques calculations for the group members.

III.SECURE NETWORK CODING TECHNIQUES AUTHENTICATION MODELS

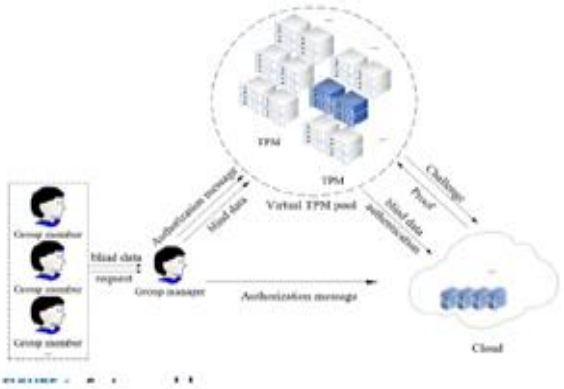


Figure 2:System Architecture

With the development of cloud computing and the popularity of smart mobile devices, people are gradually getting accustomed to a new era of data sharing model in which the data is stored on the cloud and the mobile devices are used to store/retrieve the data from the cloud. Typically, mobile devices only have limited storage space and computing power. On the contrary, the cloud has enormous amount of resources. In such a scenario, to achieve the satisfactory performance, it is essential to use the resources provided by the cloud service provider to store and share the data. the development of cloud computing and the popularity of smart mobile devices, people are gradually getting accustomed to a new era of data sharing model in which the data is stored on the cloud and the mobile devices are used to store/retrieve the data from the cloud. Typically, mobile devices only have limited storage space and computing power. On the contrary, the cloud has enormous amount of resources. In such a scenario, to achieve the satisfactory performance, it is essential to use the resources provided by the cloud service provider to store and share the data.

There are certain principles should be considered when designing a Secure Network Coding Techniques authentication protocol

1) Protocol should be designed according to the common resource features of target constrained devices such as microprocessor or microcontroller, memory, and energy

2) Avoid highly computational mathematical operation as it requires much processing which consumes a lot of power and memory .low computational overheads makes memory and power requirement at minimal

3) Authentication Messages size should be small, as the bandwidth of wireless radio is small (IEEE 802.15.4 bandwidth is 256kbps)
4) Number of messages exchanged between authentication parties should be kept at minimum
5) Cryptographic primitives used while authentication should be Secure Network Coding Techniques such as symmetric cryptography, Message Authentication Code (MAC), HASHING, XOR and AND operations

Existing System
- Mobile devices only have limited storage space and computing power. On the contrary, the cloud has enormous amount of resources.
- In such a scenario, to achieve the satisfactory performance, it is essential to use the resources provided by the cloud service provider to store and share the data.
- Development of cloud computing and the popularity of smart mobile devices, people are gradually getting accustomed to a new era of data sharing model in which the data is stored on the cloud and the mobile devices are used to store/retrieve the data from the cloud.

Disadvantages
- All existing protocols focus on the faults or dishonesty of the cloud, they have overlooked the possible the project proposesak sense of security and/or low security settings at the client.
- Existing auditing protocols are unable to work correctly.

Proposed System
- The security analysis of the scheme shows that the scheme is safe and can resist both replace attacks and replay attacks.
- The experimental evaluation of the scheme shows that the scheme can achieve Secure Network Coding Techniques calculations for group members and the TPM.

Advantages
- By introducing an efficient blind method, this paper ensures the data privacy and identity privacy of the group members.
- The security analysis of the scheme shows that the scheme is safe and can resist both replace attacks and replay attacks.
- The experimental evaluation of the scheme shows that the scheme can achieve Secure Network Coding Techniques calculations for group members and the TPM.

IV. SECURITY FEATURES FOR A SECURE NETWORK CODING TECHNIQUES AUTHENTICATION PROTOCOL

A. security requirements

when designing an authentication protocol certain security requirements must be considered, the design goal of a Secure Network Coding Techniques authentication scheme is finding a compromise between low resource requirements performance, and security strength which are discussed in this section.
1) Secure Network Coding Techniques security solution: The nodes in the Cloud resource constrained in terms of processing power, battery backup, memory, speed, etc. Hence, a Secure Network Coding Techniques security primitives solution is required.
2) Mutual authentication: all parties involved in communication authenticate each other. This is one of the most important requirements for clouds to have a secure communication.
3) Anonymity: when data is transmitted the identity of communicating parties should be hidden so that the attacker can't distinguish between user/nodes and hence can't trace user/node by their identity.
4) Scalability: to keep the network scalable the addition of new nodes should be dynamic and the system should be able to cope with this increase.
5) Confidentiality: in this requirement, the secret data transmitted between parties involved in authentication must be kept secret. only legitimate parties can get
access to it.
6) Availability: In this requirement, the server/gateway or the nodes must be continuously available to the user to access information or send commands to the nodes, as and when required.
7) Attack resistance: To guarantee secure communication within the cloud network, the authentication process should be secure against

several potential attacks, such as replay attacks, DoS attack, impersonate attack, user/node traceability attack, man-in-the- middle attacks, etc.

B. security attacks against authentication

There are some security attacks that an attacker can use to breach the security of the authentication protocol we explore some of them here

1 Denial of Service attack: The DoS attack hinders the avail- ability of a system offering services. During this attack the illegal entity consumes the resources exhaustively, thereby making the system unavailable to the legal entities. This at-tack is generally achieved by launching resource consuming activities. Such an attack becomes vital for constrained devices in cloud networks, where the resources are already limited.
2 Impersonation attack: This attack occurs when an illegal user or node pretends to be a legal entity by replaying a genuine message intercepted from a previous successful communication.
3 Man-in-the-middle attack: This attack occurs when the adversary silently listens to the communication of two legal parties with the intent to delay, alter or delete messages exchanged during communication. Such attacks are mostly present within the context of Public-Key Cryptography (PKC). In case of PKC, the adversary does not try to break the keys of the communicating parties, rather it tries to become the falsely trusted man-in-the- middle. This is achieved by replacing the exchanged session key with its own. Thereby each of the parties establishes a secure channel with the adversary, who gains access to messages in plaintext.
4 Smartcard stolen/breach attacks: The user's smart card is a tamper-resistant device. If the smart card of a user is lost or stolen, an attacker can retrieve all the sensitive information stored in the stolen smart device's memory
5 using the power analysis attack. Then, using this retrieved information, the attacker can retrieve other secret information of the communicating parties.
6 Eavesdropping attack: It refers to the process of listening to an ongoing communication, which is an initial step for launching the other attacks. Such attacks are easier to perform on unprotected wireless channels, because the communication takes place in an open insecure wireless channel.
7 Privileged insider and stolen-verifier attack: In this attack an attacker or a privileged but malicious user could gather sensitive user information (i.e. verifiers), therefore he/she could not try and impersonate a user on any other network.
8 Gateway node bypassing attack: The illegitimate entity can bypass the legal gateway node and get connected to an cloud without performing the authentication process.
9 Offline guessing attack: Any illegal entity can acquire passwords (offline guessing mode) using a "Brute-force" attack to guess the passwords.

V. SECURE NETWORK CODING TECHNIQUES SECURITY CRYPTOGRAPHIC PRIMITIVES

A. Hash Function

A hash function maps a variable-length block of data into a smaller fixed-length block. This property is very important for constrained devices some keys require to be large for security purpose therefore, storing them in hash format save a lot of memory also message size becomes smaller when message exchanged between authentication parties. The purpose of a hash function is to produce a "fingerprint" of a file, message, or other block of data [10]. The interesting part about hashing is the output which is sensitive to even a tiny change hence if an attacker tries to modify the message digest(output) the output completely changes therefore, the integrity of the hash message is guaranteed in figure[3] there are some Secure Network Coding Techniques hash algorithms with their memory and energy consumption [11].

Table 1:Secure Network Coding Techniques Hash functions and its characteristics

Algorithm	Area (GE)	Mean Power (µW)	Technology (µm)
Spongent	738	1.57	0.13
Photon-80	865	1.59	0.18
Keccak	1,300	-	0.13
U-Quark	1,379	2.96	018
D-Quark	1,702	3.95	0.18
S-Quark	2,296	5.53	-
Armadillo2-A	2,923	44	-
Armadillo-A	3,972	69	-

B. Message Authentication Code (MAC)

A MAC is symmetric cryptography technique (sometimes called: keyed hash) takes two inputs, a message and a secret key which is shared between the authentication initiator and the authentication responder only. By using a secret key, a MAC allows the recipient of the message to not only verify the integrity of the message, but also authenticate that the sender of the message who has the shared secret key. If a sender doesn't know the secret key, the hash value would then be different, thus allowing the recipient to see the message was altered.

VI. CONSTRUCTING A SECURE NETWORK CODING TECHNIQUES AUTHENTICATION SCHEME

The first step in designing a Secure Network Coding Techniques authentication scheme is to choose the right security primitives with respect to the target system how to use such primitives for building an efficient, secure and robust authentication and key management protocol with the Cloud network constrained devices requirement.

There are two broad categories used for constructing a Secure Network Coding Techniques authentication

A. Using Symmetric-key Infrastructure (SKC)

Symmetric cryptography approach is more preferable as it can easily implemented for constraint network such cloud networks, it is efficient in term of computational time and less complicated on mathematical operation, it takes only few milliseconds and can be run on memory restricted microcontroller with ram less than 1KB[12]. In symmetric-based authentication a single key is shared between authentication entities.

There are two types of symmetric-base authentication the first one is to use one of the well-known symmetric cryptography algorithms such as Advance Encryption Standard algorithm (AES) or Data Encryption Standard (DES).

The message exchanged during the authentication phase are encrypted using a key which is known in advance between the authentication entities.

MAC is implemented with a combination with these symmetric algorithm to provide authentication and integrity for the message exchanged between the sender and the receiver. Essentially, a MAC is an encrypted checksum generated on the underlying message that is sent along with a message to ensure message authentication.

The second method is using hash function and logical XOR operation. In this method no encryption/decryption algorithm is used, instead a cryptographic one- way hash function and XOR are used as in figure [4]. This method is secure and computationally lighter in term of memory and energy. In [13] an experiment was conducted the approximate running time used for computing hash function is ≈ 0.0004 ms where the time used for computing symmetric encryption/decryption is ≈ 0.312 ms. This experiment was performed using the AES symmetric encryption/decryption function, and the SHA- hash function. The result of comparison between different symmetric authentication protocols in Table(2) shows that the time of schemes using hash and XOR is more Secure Network Coding Techniques than other schemes using AES. The hash method works well with constraint network such Clouds in which devices are battery powered and memory is limited.

Most of the recent work in Cloud authentication schemes [2,3,4,14,15] Symmetric cryptography approach is used as its secure, fast and consume less energy the only problem is the key management and memory needed for storing these keys but this problem was solved by delegating key storing to the gateway node as it can be considered as powerful fully function device (FFD) which have constant energy and enough memory [4].

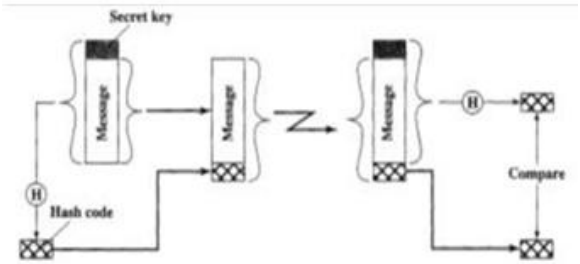


Figure 3:Message authentication using one-way hash function

B. Using Public Key-infrastructure (PKI)

Conventional PKI authentication techniques have a flexible key management but modular multiplication and squaring of large integers consumes a significant amount of microcontroller power and memory. The number of handshakes and size of the messages

exchanged during authentication with constrained devices should be kept at the minimum. In particular, transmission of long messages containing conventional X.509 certificates yields a sizeable airtime consumption, a significant latency in the authentication protocol when running over a typical low-rate communication channel[16].

there are several methods used in literature to perform a secure authentication using PKI. RSA and ECC are two public key algorithms used for authentication. ECC offers smaller key size, faster computation as well as memory, energy and bandwidth saving and better suited to small devices than RSA Using Digital Signature: Similar to MACs, digital signatures append an authentication tag to a message. The crucial difference between digital signatures and MACs is that digital signatures use a pair of keys public and private for both generating the authentication tag(signature) and verifying it. Most digital signature authentication schemes are implemented with the help of a hash function. Also, they are usually slower than MACs. Digital signature generation involves two steps. The first step is of hashing the authentication message and in the second step the hashed

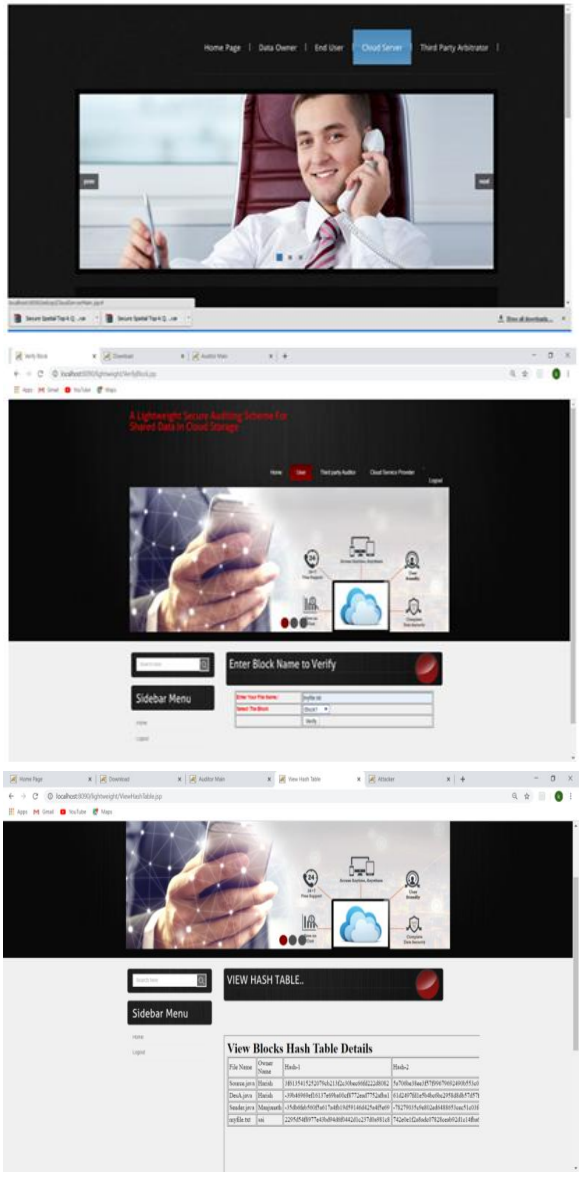
Table 2:Comparison of computational cost between Symmetric protocols

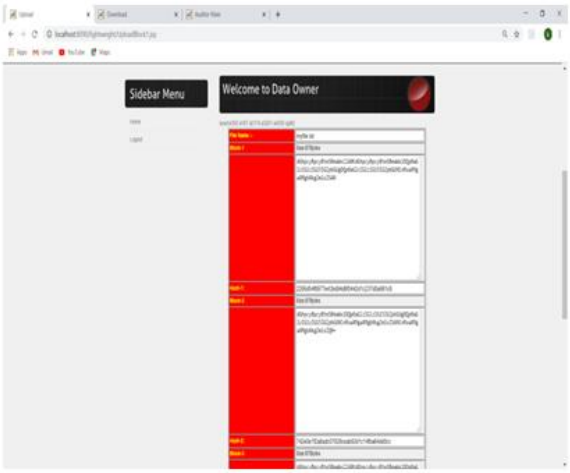
[4]					ms
Farash et al. [14]	11 T_h	7 T_h	14 T_h	32 T_h	0.0128 ms
Das et al. [18]	5 T_h +1 $T_{(d/e)}$	-	5 T_h +4 $T_{(d/e)}$	10 T_h +5 $T_{(d/e)}$	0.6555 ms
Khan and Alghathbar [19]	4 T_h	2 T_h	6 T_h	12 T_h	0.0048 ms
Turkanovic and Holbl [20]	4 T_h +1 $T_{(d/e)}$	-	7 T_h +5 $T_{(d/e)}$	3 T_h +4 $T_{(d/e)}$	0.5224 ms
Huang et al.[21]	4 T_h	1 T_h	6 T_h	11 T_h	0.0044 ms
R.Amin et al.[3]	12 T_h	5 T_h	15 T_h	32 T_h	0.0128 ms

Th – time for a hash operation; TD/E – time for symmetric-key decryption/encryption

value(message digest) is signed using the sender private key .This second step produces a value (the 'signature') that is attached to the message. using Digital Certificate: In [17] proposed PKI authentication and key agreement protocol for Clouds which provides authentication without any explicit signature The author has used a combination of elliptic curve Diffie-Hellman (ECDH) for key agreement protocol and “implicit” certificate Elliptic Curve Qu-Vanstone (ECQV) this combination found better than the traditional schemes relying on explicit X.509 certificates. 13 packets needed for the 725 bytes of the explicit X.509 certificate in the Privacy Enhanced (PEM) format, or the 9 packets required to send the 495 bytes of the explicit X.509 certificate in the Mail Distinguished Encoding Rules (DER) format While relying on a standard and widely accepted ECDH scheme, it significantly improves airtime savings by employing implicit ECQV certificates. usage of implicit certificates always ensures the maximal airtime saving, with performance gains over explicit X.509 PEM certificates ranging from 77,1% to 86,7%, and from 50,9% to 84,7% with respect to the explicit X.509 certificate in the (DER) format.

Result





VII. CONCLUSION

Cloud computing is an emerging technology, security and authentication is a center focused topic in cloud infrassstruture. we have analyzed the main approaches to the design of Cloud uses Secure Network Coding Techniques authentication protocols and the constraints of their use. Symmetric-key infrastructure schemes are fast, secure and doesn't consumed much processing power but they require complicated key management, on the other hand, public-key infrastructure schemes have a flexible key management but consume much computational time and memory space. ECC prove its strength and reliability with constrained networks. Various cloud devices have small memory, restricted to certain power limits and computational capability hence PKI approach require to be improve to be adapted with cloud environment.

REFERENCE

[1] Babar S, Mahalle P, Stango A, Prasad N, Prasad R. Proposed security model and threat taxonomy for the internet of things (Cloud). In: Recent trends in network security and applications. Springer Berlin, Heidelberg; 2010. p. 420–9. doi: 10. 1007/978-3- 642- 14478- 3 _ 42.

[2] P.K. Dhillon, S. Kalra, A Secure Network Coding Techniques biometrics based remote user authentication scheme for Cloud services, Journal of Information Security and Applications (2017),http://dx.doi.org/10.1016/j.jisa.2017.01.003

[3] R. Amin et al., Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks, Computer Networks (2016), http://dx.doi.org/10.1016/j.comnet.2016.01.006

[4] M. Turkanovic´ et al., A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion, Ad Hoc Netw. (2014), http://dx.doi.org/10.1016/j.adhoc.2014.03.009

[5] JingLiu et al," Internet of things' authentication and access control", Int. J. Security and Networks, Vol. 7, No. 4, 2012

[6] Savio Sciancalepore et al,' Public Key Authentication and Key agreement in Cloud devices with minimal airtime consumption', 2016 IEEE.

[7] S. Sciancalepore, A. Capossele, G. Piro, G. Boggia, and G. Bianchi.Key Management Protocol with Implicit Certificates for Cloud systems. In ACM Cloud-Sys Workshop, May 2015.

[8] K. Xue, C. Ma, P. Hong, R. Ding, A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks, J. Netw. Comput. Appl. 36 (2012) 316–323.

[9] S. Ozdemir, Y. Xiao, Secure data aggregation in wireless sensor networks: a comprehensive overview, Comput. Netw. 53 (2009) 2022–2037.

[10] http://williamstallings.com/Cryptography/CRYPTOGRAPHY AND NETWORK SECURITY sixth edition

[11] Manjulata AK. Survey on Secure Network Coding Techniques primitives and protocols for RFID in wire- less sensor networks. International Journal of Communication Networks and Information Security (IJCNIS) Vol. 6, No. 1, April 2014

[12] Jorge Granjal et al,' Security for the Internet of Things: A Survey of Existing Protocols and Open Research issues', DOI 10.1109/COMST.2015.2388550, IEEE Communications Surveys & Tutorials

[13] L. Xu , F. Wu , Cryptanalysis and improvement of a user authentication scheme preserving uniqueness and anonymity for connected health care, J. Med. Syst. 39 (2) (2015) 1–9 .

[14] M.S. Farash, M. Turkanović, S. Kumari, M. Hölbl, An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment, Ad Hoc Networks (2015), doi: http://dx.doi.org/10.1016/j.adhoc.2015.05.014

[15] Sima Arasteh et al, "A New Secure Network Coding Techniques Authentication and Key agreement Protocol For Internet of Things", 13th International ISC Conference on Information Security and Cryptology (ISCISC2016) September 7-8, 2016; Shahid Beheshti University – Tehran, Iran

[16] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk.'Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 5280, May 2008.

[17] Savio Sciancalepore et al' Public Key Authentication and Key agreement in Cloud devices with minimal airtime consumption', 2016 IEEE.

[18] A. Das, Kumar, P. Sharma, S. Chatterjee, S.J. Sing, Kanta, A dynamic password-based user authentication scheme for hierarchical wireless sensor networks, J. Netw. Comput. Appl. 35 (2012) 1646– 1656.

[19] M.K. Khan, K. Alghathbar, Cryptanalysis and security improvements of 'two-factor user authentication in wireless sensor networks', Sensors 10 (2010) 2450–2459.

[20] M. Turkanovic, M. Hölbl, An improved dynamic password- based user authentication scheme for hierarchical wireless sensor networks, Electron. Electric. Eng. 19 (2013) 109–116.

[21] H.-F. Huang, Y.-F. Chang, C.-H. Liu, Enhancement of two- factor user authentication in wireless sensor networks, in: IEEE Computer Society, 2010, pp. 27–30.