I.J. Wireless and Microwave Technologies, **2021, 5, 35-42**
Published Online October 2021 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2021.05.05

An Efficient and Cloud Based Architecture for Smart Grid Security

Mohammad Rasoul Momeni*
Golpayegan Faculty of Engineering, Isfahan University of Technology, Iran
Email: m.momeni@of.iut.ac.ir

Fatemeh Haghighat
Golpayegan Faculty of Engineering, Isfahan University of Technology, Iran
Email: f.haghighat@of.iut.ac.ir

Mohsen Haghighat
Great Tehran Electricity Distribution Company, Tehran, Iran
Email: mhaghighat520@yahoo.com

Received: 20 August 2021; Accepted: 24 September 2021; Published: 08 October 2021

Abstract: Due to explosive growth of users, increasing energy demand and also the need to improve efficiency and maintain the stability of the electricity grid, smart grid is the only option available to electrical industry engineers. In fact, the smart grid is a physical-cyber system that provides coherent and integrated communication, processing and control functions. The smart grid provides control and management of millions of devices in the electricity industry in a reliable, scalable, cost-effective, real time and two-sided manner. Given the increasing growth of cyber threats in the last decade, the need to protect the electricity industry and its critical systems seems essential. The slightest disruption to the power industry's systems results in disruption to other industries, reduced productivity, and discontent. Hence we proposed an efficient cloud based architecture to improve smart grid performance. Proposed architecture provides data security and privacy against different types of cyber threats such as replay attack, modification attack and so on.

Index Terms: Smart grid, cloud computing, security, privacy, cyber threats

1. Introduction

Changes in requirements in the electricity industry such as the need for higher efficiency, network stability, optimal device management, significant increase in data volume, comprehensive data security, etc. led to the transition from traditional network to smart grid. In the smart grid, continuous network monitoring is performed intelligently and in real time, so the slightest disturbance is easily detected and acted upon. In this network, a huge amount of data is generated, which is done by using cloud computing technology, storage and processing of data in a desirable way [1]. Cloud computing technology with its unique specifications has created great revolution in Information technology [2]. In fact, cloud computing means easy, demand-based network access to a shared repository of processing and reconfigurable resources such as network, server, storage space, applications and services [3]. Another noticeable advantage of cloud computing technology is virtualization. It can be implemented at different levels of the network, operating system, etc., and while increasing productivity, reduces costs by reducing hardware dependence [4]. There are multidirectional and two-way communications in the smart grid between different devices. It makes responsiveness, which is one of the most substantial requirements of the smart grid, achieved. Another outstanding requirement of smart power grid is high accessibility, which is provided by cloud computing technology. It is important to protect data against cyber threats. Some of these threats are as follows:

- Impersonation: when an adversary presents him/herself as an authorized user.
- Data modification: adversary aims to change data, as a result data integrity is violated and wrong decisions will be made.
- Disclosure of data: adversary can access to data that usually are not able to access. It means disclosure of data to unauthorized users [5].

Generally, our common threats in this field can be divided into two categories:

- Internal threats from cloud service providers.
- External threats from hackers and adversaries.

It is necessary to meet several requirements to prevent the occurrence of these threats. Some of the most vital requirements are as follows:

- Providing efficient authentication service
- Data integrity
- Providing confidentiality service
- Providing access for legitimate users
- Users anonymity when using the platform

The rest of this paper is organized as follows: Section 2 provides a brief overview of related works including introduction and analysis. Section 3 describes principals of proposed scheme; Section 4 describes proposed scheme. Sections 5 and 6 represent security and performance analysis respectively. Finally, section 7 concludes the paper.

2. Related Works

In this section, top related works will be introduced and analyzed. Fang et al. Proposed a scheme to use cloud computing technology in smart grids [6]. In their method, the application of various features of cloud computing technology such as cloud storage, virtual machines were investigated in a detailed and analytical manner in the smart grid. The security of cloud computing technology was also examined in the above method. In this paper, the application of different areas of cloud computing technology is reviewed in smart grid and finally, cloud security is briefly investigated. No precise framework has been proposed to enhance the security of the smart grid and issues were surveyed generally. Demir et al. Have utilized cloud computing technology to improve the security of the smart grid [7]. They specifically concentrated on distributed denial of service attack and counteracting it. In this regard, they have proposed two techniques. There is no comprehensive approach to enhance smart grid security using cloud computing technology in this paper and it focuses only on countering a specific attack. Abdul Rahman et al. examined security challenges of smart grid [8]. They classified and analyzed identified challenges based on threat sources carefully. At the end, they proposed a framework for achieving more security in the smart grid. The proposed framework is very general and vague and needs to be focused on particular domains of smart grid. In fact, the authors did not provide a specific solution and technique. Shrestha et al. proposed a methodology called Smart Grid Security Classification (SGSC) developed for complex systems such as the smart grid, focusing on the specifics of Advanced Metering Infrastructure (AMI) systems [9]. They covered risk analysis methods, security criteria and protection mechanism in their methodology. In this scheme, a system is assigned to a security class based on factors like protection mechanism which is implemented. Their methodology does not support automatic computation of scores and multi-metrics approach.

3. Principals of Proposed Scheme

In this section, principals of proposed scheme will be investigated.

3.1 Architecture of Cloud based Smart Grid

In this section, architecture of our private cloud based smart grid is depicted. Security is a crucial factor to apply private cloud. The data stream in the proposed architecture is transmitted through optical fiber infrastructure, which, in addition to high reliability, also ensures high transmission speed. It should be noted that in Figure 1 straight and two-way lines represent the flow of information and lines have a curvature and one direction represent the electricity.

3.2 Storage in Cloud based Architecture

In smart grid, there is exponential growth of data from different sources such as transmission network, distribution network, smart meters and so on. Also this huge amount of data must be processed and analyzed quickly. Without the use of cloud computing technology, such tasks are very difficult and slow to perform. Utilizing cloud computing technology provides unlimited storage space. Also, powerful servers in the cloud environment can process and analyze this huge amount of data quickly, and as a result, real-time control of various devices in different environments is easily possible. Another important advantage of cloud storage is its high fault tolerance due to server redundancy. Cloud storage ensures data security through integrated management and backup in different locations [10]. For example, dispatching centers at different levels can back up and manage their data on different servers. In this scenario, if a center

encounters cyber-attacks, it can simply start working with the backed up data after repelling the attack. In short, cloud storage is intelligent, automated and distributed which is a wonderful development.

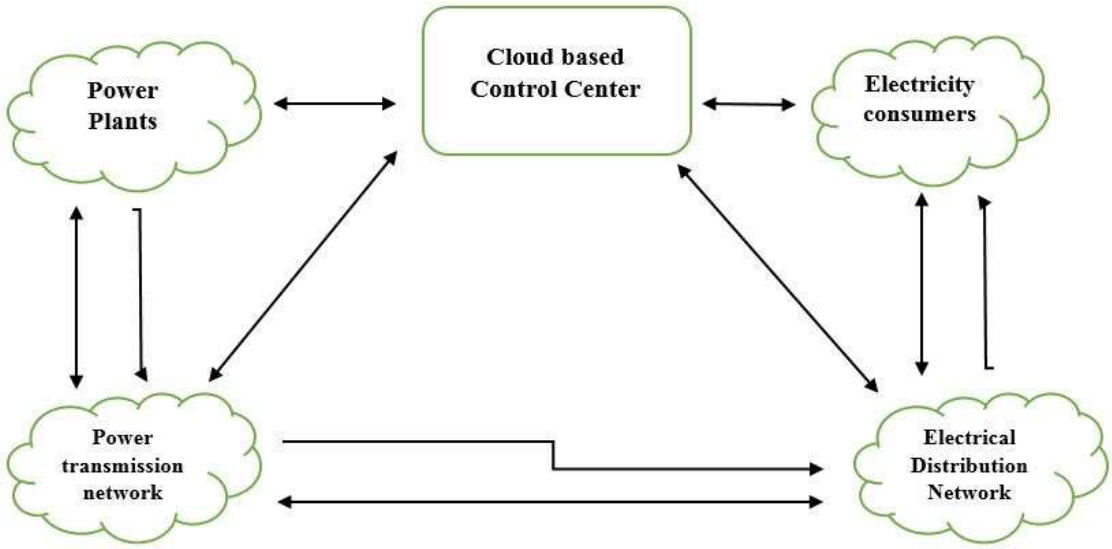

Fig. 1. Architecture of private cloud based smart grid

3.3 Virtualization in cloud-based architecture

The use of virtualization technology at different levels of the network, operating system and virtual machines for different smart grid systems leads to increased efficiency and a significant reduction in costs by reducing hardware dependence. In the last decade, virtualization has been increasingly adopted by organizations and companies as a reliable way to reduce costs [11]. For example, China Shenzhen Power Supply Company was able to set up 60 virtual servers with only 4 physical servers in 2009 by virtualization technology and reduced its energy consumption by up to 90% [12].

3.4 Security in cloud-based architecture

Integrated cloud computing management is one of the key factors in providing data security. Cloud computing technology also dramatically improves time factor in disaster recovery scenarios. The reason for this improvement is cloud computing features such as high availability, high reliability and distribution [13].

3.5 Basics of cryptography

Due to use of elliptic curve cryptosystem, in this section we will provide a brief description of this method. The elliptic curve cryptosystem, developed independently in 1985 by Neil Koblitz [14] and Victor Miller [15], and now it is an integral part of modern cryptography. Since its presentation, a lot of research has been done in this regard and all of which prove its high computational efficiency. The smaller key size feature for the elliptic curve cryptosystem has advantages such as high speed and optimal power consumption, bandwidth and storage space. In addition to these advantages, there is a high level of security for this method compared to other asymmetric cryptographic methods. In an elliptic curve cryptosystem (based on discrete logarithm problem on elliptic curve), a 160-bit key is capable of providing security equivalent to a 1024-bit key in the RSA cryptosystem (based on integer factorization problem) [16]. The sum of these features has led us to use this superior encryption technique in scenarios where we need to create higher security. Therefore, it is the best option for providing security in smart grid based on cloud computing technology. In addition, with its standardization, it is also used in many commercial products today.

The security of an elliptic curve cryptosystem depends on the difficulty of solving elliptic curve discrete logarithm problem (ECDLP), which is defined as: If P and Q are points on an elliptic curve and have relation ($Q = nP$), Then, knowing the two points P and Q, it is very difficult to find the value of n in practice. An important point about the elliptic curve discrete logarithm problem is that there is no direct relation to its calculation and only trial and error must be applied to solve it. As a result, the security of cryptographic systems based on elliptic curves is in the absence of a direct relationship to calculate the elliptic curve discrete logarithm problem. Another salient issue that needs to be mentioned in this section is the Computational Diffie-Hellmann Problem (CDHP), which is defined as: If we have (P, aP, bP) then it is very difficult to calculate (abP). It will be used to prove the security of the proposed scheme. The symbols used in the proposed security framework are given in Table 1.

Table 1. Symbols

ID_U	User Identity	$AK_U = S.Z_U$	Authentication Key
PW_U	User Password	$Z_U = PW_U.P$	Password Verifier
S	Server Private Key	TID_U	User Dynamic Identity
$Q = S.P$	Server Public Key	P	Base Point
‖	Concatenation Operator	$H()$	Hash Function
n_1 , n_2	Random Numbers	$E_{AK}()$	Symmetric Encryption Function

4. Proposed Scheme

In this section, a cloud security framework based on the elliptic curve cryptosystem will be presented to protect data security and privacy in the smart grid.

4.1 Registration Phase

At this stage, the user registers through a secure channel. Note that this step is done only once, while the authentication step can be repeated many times. After the successful completion of this stage, the next stage, i.e. authentication, can take place. The details of this step are as follows:

1. User sends its identity and password verifier to authentication server through secure channel.
2. The server verifies the user's submitted identity and, if such an identity is available in its database, rejects the registration request. The server informs user that the registration operation must be performed with a unique and non-repetitive identity. In this way, identity management operation is performed properly. If the identity sent by the user is not duplicated, the server generates the authentication key as $AK_U = S.Z_U$. In addition, the user's identity along with the password verifier and *status* bit are stored in a table called User table.
3. The server then sends the authentication key to the user.

The status bit represents the user status. That is, if the user is logged in, the status bit will be equal to one. Otherwise its value is zero. An example of a user table is given in Table 2.

Table 2. Users Table

Identity	Password Verifier	Status Bit
ID_α	$Z_\alpha = PW_\alpha.P$	0/1
ID_β	$Z_\beta = PW_\beta.P$	0/1
ID_π	$Z_\pi = PW_\pi.P$	0/1

4.2 Mutual Authentication and Session Key Agreement

Whenever a user wants to use cloud resources, he/she has to authenticate him/herself to the server through the following steps. Of course, the user can also authenticate the server, i.e. the authentication process is two-way.

1. The user logs in with username and password then generates a random number n_1 and calculates $R = n_1.Q$ and also $M = n_1.PW_U.P$. Next user generates dynamic identity to protect real identity as follows: $TID_U = ID_U \oplus H (AK_U \| R)$. User sends $L_1 = (TID_U, E_{AK} (R, M), H (TID_U, E_{AK} (R, M)))$ to the server.

2. After receiving L_1, authentication server computes $H^* (TID_U, E_{AK} (R, M))$ then examines $H = H^*$ for detecting modification attack. If these two values are equal, the occurrence of the modification attack is eliminated, but if these they are different, the modification attack occurs and the authentication server cancels this session at this stage. Canceling the session and rejecting the authentication request will prevent denial of service attack. If the attack is not detected, the authentication server obtains R and M by decryption. It is important to note that by performing the decryption operation, the user identity is confirmed for the server since the contact is the same user who was provided with the authentication key during the registration process and he/she was able to encrypt his desired parameters. In the same step, the authentication server determines the main identity of the user based on the dynamic identity as follows: $ID_U = TID_U \oplus H (AK_U \| R)$. After obtaining the original identity, validates it through the identities in the users table. Now the authentication server generates n_2 and calculates $N = n_2.Q$. finally, the authentication server sends $L_2 = ((M+N), H (M))$ to the user.

3. After receiving L_2, user calculates N from M+N-M then computes H (N) and examines $H = H^*$ to detect modification attack. If they are not equal, current session will be aborted hence denial of service attack is eliminated. User generates $L_3 = (TID_U, H (M \| N))$ and session key as follows: $SK = n_1.PW_U.N = n_1.PW_U.n_2.S.P = n_1.n_2.S.P.PW_U$.

4. After receiving L_3, authentication server calculates $H^* (M \| N)$ and then compares it by received $H (M \| N)$ for detecting modification attack. If they are not equal, current session will be aborted thus denial of service attack is eliminated. Now authentication server generates session key as follows: $SK = n_2.S.M = n_2.S.n_1.PW_U.P = n_1.n_2.S.P.PW_U$. It is important to note that session key changes in each session. Each key is valid only for that particular session. After

agreeing on a session key, both parties use this key to encrypt sent messages and have a secure connection. After successful authentication, users request required data.

4.3 Password Change Phase

Enabling users to change their password ensures a high level of security and user friendliness of the proposed scheme. It is better to design the password change phase without interfering with the remote authentication server to have high efficiency and security. In the proposed scheme, after selecting a new password and calculating the verifier for it, user sends only the password verifier to the authentication server. Note that communication channel is secure. The steps of this phase are as follows.

1. User sends his/her identity and password verifier with a password change request to the authentication server.
2. After verifying the received identity, if user is a legitimate one, authentication server calculates H ($ID_U \| SK$) and sends it to user.
3. User calculates H^* ($ID_U \| SK$) and compares it by H ($ID_U \| SK$). If they are equal, then computes password verifier for it as follows: $Z^*_U = PW^*_U.P$. User sends this password verifier to the authentication server to replace old password verifier. Finally, a new authentication key will be generated by authentication server.

4.4 User Eviction Phase

It is possible to expel the offending users by the authentication server in the proposed scheme. For this purpose, the authentication server must remove the row related to users from the users table. If fired users attempt to log in, they will fail. The reason is that identity management will be conducted in the second step of the mutual authentication and session key agreement phase. Hence authentication server will understand these identities do not exist in the users table. As a result, dismissed users cannot login to our cloud based platform.

5. Security Analysis

In this section, security features of our cloud based platform will be investigated.

5.1 Modification Attack Resistance

A collision-free one-way hash function has been used to avoid a modification attack. If the enemy sends a modified message, the recipient simply detects the change by examining the values of the two hash functions.

5.2 Replay Attack Resistance

The proposed scheme uses a random number mechanism to prevent a replay attack. It is very difficult for the enemy to guess the values of random numbers, because they are updated and changed in each session and every time. In fact, they are one-time random numbers.

5.3 Password Guessing Attack Resistance

This attack is one of the most prevalent attacks on password-based authentication schemes [17]. One of the reasons could be the tendency of users to choose a weak password, which is also very easy to guess for hostile people. In the proposed scheme, what is used by the server and stored in the users table is not a password but a password verifier. Extracting a password from its verifier is equivalent to solving a discrete logarithm problem on an elliptic curve, which is very difficult in practice and takes thousands of years with current computing systems [18].

5.4 Stolen Verifier Attack Resistance

Our cloud based architecture is robust against stolen verifier attack since server does not store any secret table or any pre-shared secret key. Hence adversaries cannot obtain any valuable information through this attack.

5.5 Server Spoofing Attack Resistance

Our cloud based architecture provides mutual authentication for both participants. User authenticates the server and server can authenticate the user. In more detail, the adversary does not know the value of the server private key. Therefore, authentication key cannot be obtained. Not having an authentication key means not being able to decrypt and obtain R and M in the second step of the mutual authentication and session key agreement phase. Also, in the absence of authentication key, it is not possible to calculate the real identity of the mobile user (ID_U).

5.6 Insider Attack Resistance

A client CL may register with servers S_1, S_2 and so on using a common password pw and the identity id for convenience. if the privileged-insider U_1 of S_1 has the knowledge of CL's pw and id, then U_1 may try to access other servers S_2, S_3 and so on by using the same pw and id. In our cloud based architecture, the authentication server only

stores password verifier and extraction of password is very complicated due to hardness of elliptic curve discrete logarithm problem (ECDLP).

5.7 Known Session Specific Temporary Information Attack Resistance

The attack states that if temporary and secret information of a particular session is disclosed, the security of the session key will be compromised. In the proposed scheme, if random numbers are disclosed, the session key will not be exposed, because in the generation of the session key, other components such as the user password and the server private key have been used that the enemy does not know. On the other hand, to calculate the session key, the enemy must calculate the PW_U.S.P from the pair (PW_U.P, S.P), which is equivalent to solving the computational Diffie-Hellman problem. As mentioned before in the section basics of cryptography, solving this problem is very difficult in practice.

6. Performance Analysis

In this section, performance features of our proposed cloud based architecture will be presented.

6.1 No Clock Synchronization Problem

Many of the proposed authentication schemes use the time stamp mechanism to prevent replay attacks. However, it should be noted that the time stamp mechanism has a high operating overhead in distributed systems [19]. In order to avoid this high operating overhead and also the user-friendliness of the proposed scheme, random numbers have been used in the proposed cloud based architecture.

6.2 Low Bandwidth

The proposed scheme is implemented using an elliptic curve cryptosystem, which has the shortest key length among all types of asymmetric encryption methods. In addition to having high speed, it leads to use less bandwidth. In addition, in part of the proposed platform, symmetric cryptography is used. It is important to note that in this case, the encrypted text is generated with a smaller number of bits. As a result, messages exchanged in this way are shorter in length and therefore have lower bandwidth requirements and communication costs.

6.3 Identity Management

In the registration phase of our proposed scheme, non-repetition of the sent identity will be checked. Also in the second step of the mutual authentication and session key agreement phase, the calculated identity is validated from the dynamic identity. In this way, the identity management operation is best supported by the proposed architecture.

6.4 User Anonymity

User anonymity means protection of privacy and is raised in front of the public, not the relevant server [20]. This is because the server must identify and authenticate the user in order to provide audit services and operations. Our proposed cloud based platform satisfies user anonymity, because in the registration and password change phases that real identity transmits, the channel is secure. Also in the mutual authentication and session key agreement phase that channel is not secure, dynamic identity transmits instead of transmission real identity.

6.5 Scalable and Fast

Using an independent authentication center makes our scheme scalable, in which case there will be no additional processing on the server. Also, using elliptic curve cryptosystem, which has a high speed due to its smaller key size, has made the proposed scheme fast and user-friendly.

6.6 Session Key Agreement

In our proposed cloud based platform, a session key is generated which uses random numbers. This session key provides secure communications over open channels by encrypting the exchanged messages and ease of operation.

6.7 Password Change Phase

Our proposed scheme supports Password change operation, hence this platform is more secure than other proposed platforms. In addition, the user can change password without any intervention from authentication server. This property brings high security and user friendliness for our proposed cloud based architecture.

7. Conclusion

In this paper, an efficient architecture based on cloud computing technology is presented to improve security in the smart grid. For reasons such as significant growth of subscribers, increasing energy demand and also the need to increase productivity and maintain the stability of the electricity grid, today the smart grid is the only way to properly

manage the power grid. The proposed architecture with the benefit of the features of cloud computing technology, while having high efficiency, is able to provide security and privacy of data against various types of cyber-attacks such as replay attack, modification attack, etc. In the proposed architecture, an elliptic curve cryptosystem is used, which in addition to ensuring more security, has a smaller key length and consumes less bandwidth. Security and performance analysis confirms the claim that while ensuring high performance, the security of the proposed architecture is excellent and resistant to various cyber-attacks. In future, we aim to research about secure storage and integrity of smart grid data using cloud computing technology.

References

[1] Rashid G. Alakbarov, "Challenges of Mobile Devices' Resources and in Communication Channels and their Solutions", International Journal of Computer Network and Information Security(IJCNIS), Vol.13, No.1, pp.39-46, 2021. DOI: 10.5815/ijcnis.2021.01.04

[2] M. R. Momeni, F. Haghighat. "An Ultra Lightweight and Secure Architecture for Mobile Commerce Using Cloud Based Mobile Agents". Journal of Network and Innovative Computing, ISSN 2160-2174 Volume 6 (2018) pp. 034-040.

[3] P. Mell, T. Grance, The NIST definition of cloud computing (draft), 2011, Available: http://csrc.nist.gov/publications/drafts/800–145/Draft-SP-800-145_cloud-definition.pdf

[4] Momeni, M. R. (2015). A Survey of Mobile Cloud Computing: Advantages, Challenges and Approaches. International Journal of Computer Science and Business Informatics, special issue: 15(4), 14-28.

[5] Momeni, M. R. (2015). An Efficient Authentication Protocol for Mobile Cloud Environments using ECC. International Journal of Computer Science and Business Informatics, Special Issue: 15(4), 29-39.

[6] B. Fang, X. Yin, Y. Tan, C. Li, Y. Gao, Y. Cao, J. Li, "The contributions of cloud technologies to smart grid", Renewable and Sustainable Energy Reviews, Vol. 59, pp. 1326-1331, June 2016. (doi:10.1016/j.rser.2016.01.032).

[7] K. Demir, H. Ismail, T. Gurova, N. Suri, "Securing the cloud-assisted smart grid", International Journal of Critical Infrastructure Protection, pp. 100-111, Dec. 2018. (doi:10.1016/j.ijcip.2018.08.004).

[8] A. O. Otuoze, M. W. Mustafa, R. M. Larik, "Smart grid security challenges: Classification by sources of threat", Journal of Electrical Systems and Information Technology, Vol. 5, No. 3, pp. 468-483, Dec. 2018. (doi:10.1016/j.jesit.2018.01.001).

[9] Shrestha.M, Johansen.Ch, Noll.J, Roverso.D, A Methodology for Security Classification applied to Smart Grid Infrastructures, International Journal of Critical Infrastructure Protection, 28 (2020).

[10] Wang. M, Zhang. Q, Optimized data storage algorithm of IoT based on cloud computing in distributed system, Computer Communications, Volume 157, May 2020, pp. 124-131. (doi: https://doi.org/10.1016/j.comcom.2020.04.023).

[11] Alboaneen. D, Tianfield. H, Zhang. Y, Pranggono. B, A metaheuristic method for joint task scheduling and virtual machine placement in cloud data centers, Future Generation Computer Systems, Volume 115, February 2021, Pages 201-212. (doi: https://doi.org/10.1016/j.future.2020.08.036).

[12] T. Li," How to build the virtual system in power enterprise information system", Electr. Power Inf. Technol, 2009.

[13] Z. Hua, Z. Nan, "Cloud computing based data storage and disaster recovery", Proceeding of the IEEE/ICFCSE, 629-632, Aug. 2011 (doi:10.1109/ICFCSE.2011.157).

[14] N. Koblitz, "Elliptic curve cryptosystem", Journal of Mathematics Computation, Vol. 48, No. 177, pp. 203-209, 1987.

[15] V. Miller, Use of elliptic curves in cryptography, Advances in Cryptology, pp. 417-426, 1985.

[16] D. Hankerson, A. Menzes, S. Vanston, Guide to elliptic curve cryptography, New York, USA: SpringerVerlag, 2004.

[17] Hafizul, & Biswas. (2013). Design of improved password authentication and update scheme based on elliptic curve cryptography. Mathematical and Computer Modelling, 57, 2703–2717.

[18] Adil Bashir, Sahil Sholla, " Resource Efficient Security Mechanism for Cloud of Things", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.11, No.4, pp. 41-45, 2021.DOI: 10.5815/ijwmt.2021.04.05

[19] R. Baldoni, A. Corsaro, L. Querzoni, S. Scipioni, S. Piergiovanni, "Coupling-based internal clock synchronization for large-scale dynamic distributed systems", IEEE Trans. on Parallel and Distributed Systems, Vol. 21, No. 5, pp. 607–619, May 2010 (doi:10.1109/TPDS.2009.111).

[20] Z. Tan, "A user anonymity preserving three-factor authentication scheme for telecare medicine information systems", Journal of Medical Systems, Vol. 38, No. 3, pp. 1-9, March 2014, (doi:10.1007/s10916-014-0016-2).

Authors' Profiles

Mohammad Rasoul Momeni received the BSc degree from Payame Noor, Iran, in 2011 and MSc from the Imam Reza International University, Iran, in 2014, respectively. Currently he is an IT security architect in department of IT at Golpayegan faculty of Engineering. His current research interests are Information security and privacy, lightweight cryptography and networks security.

Fatemeh Haghighat received the BSc and MSc degree from the Allameh Tabatabai University in 2012 and 2014, respectively. Currently she is a director of welfare affairs in department of administrative at Golpayegan faculty of Engineering. Her current research interests are human resource management, strategic management and organizational learning.

Mohsen Haghighat received the BSc and MSc degree from the Islamic Azad University, South branch in 2002 and 2009, respectively. Currently he is a director of design and engineering at Great Tehran Electricity Distribution Company, Tehran, Iran. His current research interests are power system optimization, renewable energy and Protection of power systems.

How to cite this paper: Mohammad Rasoul Momeni, Fatemeh Haghighat, Mohsen Haghighat, " An Efficient and Cloud Based Architecture for Smart Grid Security", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.11, No.5, pp. 35-42, 2021.DOI: 10.5815/ijwmt.2021.05.05

