IJICTR
International Journal of Information & Communication Technology Research

Volume 15- Number 4 – 2023 (32 -40)

Improving the Security of Management Software of Smart Meters Networks

Mahdiyehsadat Mirsharifi
Computer Engineering Department,
K. N. Toosi University of Technology,
Tehran, Iran
mah.mirsharifi@email.kntu.ac.ir

Fatemeh Rezaei*
Computer Engineering Department,
K. N. Toosi University of Technology,
Tehran, Iran
frezaei@kntu.ac..ir

Received: 20 September 2022 – Revised: 16 October 2022 - Accepted: 4 March 2023

***Abstract*— Reading traditional meters is always time-consuming and expensive. Using smart meters solves most of the problems existing in the traditional meter network. Smart meters are an advanced form of traditional electro-mechanical devices that can measure energy consumption in real-time and communicate through one or more wired or wireless networks. These devices can communicate from long distances and get changed, making them an easy target for attacks. This paper studies the security mechanisms in smart meters networks and suggests some security solutions in such networks. We have developed software for managing the information of smart meters and controlling them remotely. In this paper, we present the implemented security mechanisms in the developed smart meter management software. The proposed solutions for enhancing the security of this software include implementing the authentication system, enabling user management, and defining different access levels to prevent users from connecting without proper authentication and access control in the developed software. Moreover, hashing the password with a random salt technique is implemented for securing the database. Furthermore, we have secured the software platform to prevent web attacks such as Clickjacking and CSRF attacks.**

Keywords: Internet of Things, Smart Meters, Management, Security, Authentication.

Article type: Research Article
© The Author(s).
Publisher: ICT Research Institute

[Downloaded from journal.itrc.ac.ir on 2024-05-16]

[DOI: 10.61186/itrc.15.4.32]

I. INTRODUCTION

With technological advancements and the expansion of the use of devices related to the Internet of Things and smart homes, the issue of the security of these devices has become more urgent. To establish the security of these devices and related software, in addition to examining the methods of preventing attacks on them, we need to assess the security weaknesses in these devices to correct them and prevent them from being infiltrated and attacked. Despite of many advantages of these devices, the priority of profitability and reducing the time to provide products for the companies' market, as well as the lack of laws related to these devices, have caused manufacturers to ignore security issues and design vulnerable devices which have many security holes making them easy attack targets[1]-[3].

Smart meters are an advanced form of traditional electro-mechanical devices that can measure energy consumption in real-time and communicate through one or more wired or wireless networks. They have digital displays to show energy consumption to

* Corresponding Author

subscribers and communication units to communicate through the network to the relevant energy organization. A smart grid refers to an infrastructure that includes smart meters, communication networks, and infrastructure between smart meters and related entities, including energy consumers, energy consumption operators, energy suppliers, and consumption control systems [4]-[6].

Our only concern will not be smart meters security but also the connected network and each device used in the smart grid. We have developed smart meter management software that monitors and collects data from the smart meter network [7]. In this paper, we study the security issues of smart meter networks and investigate the vulnerabilities of smart meter management software, possible attacks, and methods to prevent these attacks.

II. Common Attacks in Smart Meter Networks

Although the Internet of Things provides significant progress in social development, economic benefits, and government activities, attackers can use it as a network for widespread cyberattacks that may cause irreparable damage. The Internet of Things connects many devices with uncertain security settings. If the mentioned devices are not secure, they can be misused, and their control can be hijacked by hackers and turned into cyber soldiers, known as bots or zombies. In general, the CIA triad or the security triangle is a respected security model that is the basis for developing security systems and policies. This trilogy includes confidentiality, integrity, and availability of information and services [8]-[10]. Each cyberattack considers one or more parts of the CIA triad, and the attacker tries to destroy that feature in the system or data. The common attacks in the IoT environment and smart meter networks [11]-[14] are as follows.

A. *Distributed Denial of Service(DDoS) Attack*

In the Denial of Service (DoS) attack, the attacker uses fake requests to involve the target system's resources and prevent it from serving. In the enhanced model of a DoS attack, the Distributed Denial of Service (DDoS) attack, the attacker sends requests from many sources. This attack affects the availability side of the security triangle. DDOS attacks include TCP SYN Flood, Teardrop, Ping of Death, and Smurf attacks. Many devices are needed to execute this attack, and IoT devices are very suitable. In the misused IoT devices for this attack, usually, the user does not realize the device has been compromised and misused by the attacker. For example, baby monitor devices and smart toys have a user interface with limited access. These devices may work even if they are attacked and become a bot and a member of the botnet network, which makes the user unaware of this happening.

B. *Eavesdropping Attack*

Such attacks destroy the user's privacy by gaining illegal access to the user's data or communication network. This attack can be implemented on a wireless communication channel or a power line. Detecting such attacks is difficult, considering the attacker tries to remain hidden. This attack is usually executed through the WAN networks.

C. *Man-in-the-Middle Attack*

In this type of attack, the attacker places himself between the communication path of the two parties and records the messages sent between the two parties. The two parties think that they are directly communicating with each other and that there is no middle person. This attack can be implemented in a LAN or WAN network. If implemented inside the local network, it can compromise the communication between the smart meter and the gateway and provide false information from the smart meter to the gateway. For example, it can inform the gateway that the amount of shared consumption is less than the actual amount. If this attack is implemented in WAN, the security and privacy of people will be compromised on a large scale. The carrier can also spoof remote commands to gateways from approved entities.

D. *Packet Injection Attack*

These attacks are performed by injecting fake packets into the network, such as wrong commands for smart meters. Packet injection attacks are typically executed over a WAN. These attacks can be used to cut off part of the energy supply network or compromise the billing process by creating false bills, causing financial losses to service companies.

E. *Replay Attack*

A replay attack occurs when an attacker eavesdrops on messages over a secure network connection and then falsely delays or resends them to mislead the receiver. This attack is more dangerous than other attacks because the attacker does not need advanced skills to decrypt the message after it is captured from the network. The attack can also succeed only by resending the entire message that has been encrypted.

F. *Malware Injection Attack*

These attacks are usually implemented by injecting malware into the WAN network to affect the communication between devices and the consumption reporting and billing process. The situation of demand and consumption in the smart energy network may be disrupted due to the instability of the consumption report.

G. *Remotely Connecting and Disconnecting Service (RCDS)*

The possibility of remotely connecting and disconnecting the service to the smart energy network, if attackers misuse it, can cause the entire network or parts to be disconnected. If this attack is executed on a large scale, it can cut off many users' water, electricity, or gas. These attacks are usually carried out through the

[Downloaded from journal.itrc.ac.ir on 2024-05-16]

[DOI: 10.61186/itrc.15.4.32]

WAN network and by injecting packets with false information.

TABLE I. TABLE I. COMMON ATTACKS IN THE SMART METERS NETWORKS

Attack	Target Security Service
DoS/DDoS	Availability
Eavesdropping	Confidentiality
Man-in-the-Middle	Confidentiality
Packet Injection	Integrity
Replay	Integrity
Malware Injection	Integrity
RCDS	Availability
Firmware Manipulation	Integrity

H. Firmware Manipulation

Firmware manipulation includes changing the metrological or non-metrological part of the smart meter or gateway. If the attacker manipulates the metrological part, it can disrupt the billing process of the target device. For example, this goal can be achieved by falsely reporting the amount of consumption. Manipulating the firmware of a meter or gateway can be done through direct physical access or the WAN network. These attacks can affect a single user but also can be carried out on a large scale. It is possible to manipulate the firmware of many gateways remotely. These attacks are summarized in Table I.

III. SECURITY MECHANISMS IN SMART METER NETWORKS

To communicate between the components of smart energy networks, including the producer, energy production location, energy transmission tools, and user, a hybrid network is needed, which includes a core network and millions of local networks. The core network is for communicating between different parts of the network and can include connection gateways for local networks and powerful and high-bandwidth routers to transfer messages to different parts of the smart grid. In this network, wire-based transmission methods such as fiber technology enable high-volume and high-speed transmissions.

Local area networks are intended to include smart meters, sensors, and smart electronic devices installed on the energy production infrastructure. These networks usually have limited bandwidth and computing power, which reduces the possibility of monitoring and protecting them. In these networks, unlike the core network, wireless transmission methods such as WiFi and ZigBee technology and cellular networks are used frequently, which are more accessible and less expensive [15]. One way to solve security problems in the smart grid is by using protocols and security methods, such as the types of encryption used in computer networks. However, it is not possible for two reasons:

1) A major part of the smart grid includes smart meters. Smart meters use light-embedded systems that have limited processing power and memory. Due to these limitations, these devices may not be able to perform the number of calculations required for some types of encryption.

2) The smart grid uses different devices from various vendors that may not follow the same security protocols.

Therefore, we should consider specific security solutions for the smart meter networks [15]-[18] as follows. These solutions are summarized in Table II.

Authentication: The identity of people and smart meters must be verified through strong authentication methods. Organizations must apply a strict access policy that allows access to the network only when the person and device are authenticated. One of the methods to authenticate the smart meters is to filter sending packets into routers based on the combination of the MAC address and IP address of the meters. There are attacks in which the hacker can change his MAC and IP and impersonate another device, but by applying a filter on these two variables at the same time, it will be more difficult for the attacker.

Malware Protection: Malware protection must be implemented in smart meters, central systems, and monitors. Smart meters should only be able to run software if the device manufacturer produced it. For this purpose, the manufacturer must place a secure memory in the meter that contains the desired keys for software validation. The smart meter can validate any installed software before running using this key. However, considering smart meters are commonly used, supporting software produced by another approved company is necessary. In order to achieve this goal, the central part of the network should be able to change the secure memory that stores the validation keys in the meters, or there should be an anti-virus on the meters to prevent malware infection. Due to the amount of memory and the low processing ability of these smart meters, it seems far-fetched.

Using Network Intrusion Detection Systems (IDS) and Network Intrusion Prevention Systems (IPS): As it is clear from the name of these systems, the goal is to detect and prevent unwanted access to the network. The implementation carried out in these systems is better to use the combination of comparing the system status with the defined normal status and the received traffic with the characteristics of each attack. These devices should be placed at the edge of the core network to prevent an attacker from accessing the core network and critical systems. One of the measures that can be taken to prevent denial of service attacks is to limit the number of packets received from each IP.

Annual Vulnerability Assessment: New vulnerabilities are regularly found in all devices an attacker can exploit. The vulnerabilities of the devices inside the smart grid should be evaluated at least annually, and necessary measures should be taken, including updating

[Downloaded from journal.itrc.ac.ir on 2024-05-16]

[DOI: 10.61186/itrc.15.4.32]

the firmware of smart meters. For more sensitive and core devices, this assessment should be done monthly.

TABLE II. SUMMARY OF SECURITY SOLUTIONS FOR SMART METER NETWORKS

Security Solutions	Recommendations
Authentication	•Authenticating based on the combination of the MAC address and IP address.
Malware Protection	•Placing a secure memory in the meter that contains the desired keys for software validation •Changing the secure memory that stores the validation keys in the meters.
Using NIDS and NIPS	• Placing IDS and IPS at the edge of the core network.
Vulnerability Assessment	• Updating the firmware of smart meters annually. • Updating more sensitive and core devices monthly.
Refrain from Wireless Communication	• Preferring cable communication technologies such as fiber or copper wire. • Separating the network of smart meters from the Internet and other shared internal networks.
Educating Users	• Providing training programs to educate employees and consumers about the best security practices for using network facilities and software.
Encryption	• Encrypting transmitted packets between smart meters and the core network using light cryptography techniques. • Using OSGP-AES protocol.

Refrain from Using Wireless Communication: Despite the cost-effectiveness of wireless communication for smart meters, cable communication technologies such as fiber or copper wire should be used to prevent the abuse of wireless network weaknesses. Considering that in Iran, unlike European countries, there is a single producer for each utility, all these meters can be directly connected to the desired organization through a cable connection. Due to the separation of the smart grid network from the Internet and other networks, including the shared internal network, many attacks can be prevented, and a secure physical communication environment can be created between the organization and smart meters.

Educating Users: In some cases, user actions can introduce new vulnerabilities in smart meter networks. For this reason, awareness and training programs should be planned to educate users about the best security practices for using network facilities and software. This user can be an organization employee or a consumer.

Encryption: Communication between smart meters and the core network must be encrypted. Cryptography is divided into symmetric and asymmetric encryption. In symmetric encryption (such as AES), the same key is used for encryption and decryption. In asymmetric encryption (such as RSA), private and public keys are used for encryption and decryption. If encryption is done with a private key, decryption will be done with a public key and vice versa. Despite being more secure and not needing a secure channel for transferring the key, asymmetric cryptography requires high computing power and cannot be used in smart meters. Symmetric encryption requires less computational processing, but it is necessary to have a secure channel for encryption key transfer between devices.

As a recommendation for the security protocol, we suggest the OSGP protocol, which is currently being used in many European countries on a large scale in smart grid projects. This protocol was developed by the OSGP Alliance and published as a standard by the European Telecommunications Standards Institute (ETSI) [18]. It follows the OSI model, and the devices that use this protocol have a frequency between 9 kHz and 95 kHz. The OSGP protocol requires using a mandatory security protocol in the transport layer called OSGP-AES-128-PSK, abbreviated as OSGP-AES. OSGP-AES provides a two-way protected communication channel between the user and the smart meter. This secure channel provides data confidentiality using AES-128-CCM encryption, data and origin integrity through authentication, and anti-replay protection using sequence numbers. OSGP-AES secures both unicast and broadcast messages. All OSGP messages are sent within the secure channel created by OSGP-AES. These messages include the reading of smart meter data, such as the amount of energy consumption, and the security of important functions, such as changing the configuration of smart meters. Since messages and communication channels are protected, encryption and two-way authentication would be established in the network, and the network would resist replay attacks. OSGP- AES is implemented in a way that uses a unique key for each device. Using unique keys means that if one of the smart meters is compromised, the key of the other meters will remain safe. OSGP-AES is specifically designed for networks with limited memory and computing power that use legacy devices. The priority considered in its design is for use in power line communication networks. For this reason, it can provide high performance while maintaining security.

In Table III, we can see the comparison between our suggested security solutions and the ones presented in [6]. Some said security measures in this paper are not discussed in the other one, such as vulnerability assessment, malware protection, and educating users. Due to this fact, these methods haven't been concluded in this comparison.

We have recommended authentication based on the MAC address and IP address combination for devices and user and passwords for users. Reference [6] suggested using a digital signature for this purpose. The

[Downloaded from journal.itrc.ac.ir on 2024-05-16]

[DOI: 10.61186/itrc.15.4.32]

digital signature may be more secure than our proposed method, but it's also pricier.

On the other hand, we recommended encrypting transmitted packets between smart meters and the core network using light cryptography techniques like OSGP-AES protocol. Reference [6] suggested application layer encryption in addition to TLS for encryption which has more overhead than our recommended method.

Moreover, we have suggested using cable communication technologies such as fiber and separating the smart-meter network from the Internet and other shared internal networks. Reference [6] suggested a gateway-based approach, where the gateway acts as a communication unit between the metering devices in the customer premises and the utility. The gateway is also responsible for ensuring the privacy of the customer.

IV. Implementing Security Measures on Smart Meters Management Software

Security mechanisms such as authentication of devices, refraining from using wireless communication, and using intrusion prevention and detection systems should be considered when implementing the infrastructure of smart energy networks. Some other issues, like encryption, are also established when implementing the infrastructure using the OSGP-AES protocol. Training users should also be planned and done periodically by organizations. Protection against malware should also be considered by the manufacturer while constructing smart meters. This paper presents the implemented security mechanisms in the Smart Meter Management Software as follows.

A. User Authentication and defining different levels of access

To prevent users from connecting without authentication in the developed software, if the user is not yet logged in to the system, any page he wants to open will be redirected to the login page, and only after logging in will he be able to check the desired section. We have also defined some restrictions for user passwords, such as containing at least eight characters, not containing only numbers, not being among common passwords, and not including user information such as name and username in the password, as illustrated in Fig. 1.

According to the usage of the program, two types of access groups named Administrators and Operators have been defined, which have different levels of access.

1) Administrators: Administrators group has full access and can see all pages. In addition to viewing meters, they can add and remove smart meters in this software. Users of this group can see different access groups and define a new one. These users can view existing users, filter them based on their access group and user type, delete a user or define a new user, as shown in Fig. 2. In addition to changing his password, the user with management access can change other users' passwords.

2) Operators: Users of this group, unlike administrators, can only view and cannot perform any action that requires adding or deleting an item from the database. This user can only change his password. The operator user can also not perform actions such as adding a new meter, deleting an existing meter, deleting the meter's data, activating or deactivating meters, and changing the time of smart meters, as illustrated in Fig. 3. Other features of the software, including the possibility of viewing meters' information and taking action to repair them, have been given to this user.

B. Database Security

In the management software, in the table where we store the login information of the system users, the password field has been hashed with SHA-256 and the random Salt algorithm to protect the users' passwords. As shown in Fig. 4, because giving an un-hashed value to the hash function always returns a fixed character string that an attacker may find using comparison, Salt is added to increase security. Salt is a random character string that is added to the beginning or the end of the desired string, which is the user's password here, and then hashed to make the attacker's work more difficult. We have added Salt to the beginning of the password before hashing it. The hashed data may be used to verify the integrity of copies of the original data without having to have the actual data itself. This is what we do when a user logs into the software. By comparing the hashed value of the user's password stored in the system and the hash obtained from the user's input password, we find out whether the password is the same or not, and if it is the same, we allow the user to log in. The hash function is irreversible, so we can freely store it in the database.

C. Securing Software Infrastructure and Establishing Security Against Common Web Attacks

This section will discuss the best case of using the Django framework to secure the software [19]-[20] and the changes that should be made after the software production process is completed. Moreover, we will discuss the changes made to the program to be safe against common web attacks.

- *Securing Software Infrastructure*

  a) Using the latest version of the technologies used: The first thing suggested for maintaining security is to use the latest version of the technologies used for developing software, including programming languages, packages, and libraries.

  b) Disabling DEBUG: Enabling DEBUG mode in the program while developing is useful. If the program crashes, it will generate a descriptive error page that includes the problem trace and metadata, including all current Django settings. This feature is a path for troubleshooting, but it can also play the

[Downloaded from journal.itrc.ac.ir on 2024-05-16]

[DOI: 10.61186/itrc.15.4.32]

role of a guide for the attacker. That is why we disabled this feature after finishing the software production.

c) Securing SECRET_KEY: This parameter is a random character string created for the cryptographic signature. This parameter is hashed in the code and must be kept safe.

d) Defining allowed hosts and domains for the software: Normally, the ALLOWED_HOSTS parameter, which defines the host and allowed domains, is empty. In this software, the restriction is placed on the host '127.0.0.1' and domain 'localhost'. If this system needs to be used in another domain, the desired domain must be added to this list. By limiting this parameter, the software becomes resistant to HTTP header attacks.

e) Using HTTPS: If we use HTTP instead of HTTPS, which uses TLS, the attacker can find all the information transferred between the server and the client, including authentication information and API codes. TLS is a protocol to create encrypted and authenticated communication between network devices. Steps have been taken to resolve the issue, including automatically converting HTTP requests to HTTPS, forcing web browsers to communicate over HTTPS only, and enabling this on subdomains in addition to the main domain.

- *Establishing Security Against Common Web Attacks*

a) Clickjacking Attack: In this attack, a malicious site puts another site inside an invisible frame. This attack tricks the user into clicking on a web page element that is maliciously invisible or masquerading as another element. We prevent this attack by disabling the possibility of using our site in any frame.

b) CSRF Attack: A CSRF attack, or single-click attack, is an attack in which an attacker tricks a user into making a web request that he did not intend to receive. The attacker often steals the user's active cookies in this way and uses them to access the site in the future. To deal with this attack, we define in the program that cookies are available only through HTTPS requests, that JavaScript is not allowed to access them, and that cookies are sent only on an HTTPS connection. We use the CSRF token to increase security. This unique token is generated for each session, request, or ID.

In Table IV, we point out the advantages and disadvantages of our implemented security methods for the Smart Meter Management Software.

V. CONCLUSION

Different attacks can threaten smart meter networks, such as DDoS attacks, replay attacks, malware injection attacks, packet injection attacks, and many others. Each attack targets one or multiple vulnerabilities. In order to secure smart grids, we should fix our vulnerabilities. For this purpose, we have suggested security solutions including authentication, encryption, malware protection, annual vulnerability assessment, and using network intrusion detection and prevention systems. Some are related to smart grid infrastructure security, while others are related to smart meter management software security. Our course of action for securing the smart meter management software is implementing user authentication, defining different levels of access for users, establishing database security, securing software infrastructure, and dealing with the most common web attacks.

TABLE III. COMPARISON OF THE SECURITY SOLUTIONS FOR SMART METER NETWORKS

Security Solution	This Paper	[6]	Comparison
Authentication	Authentication based on the MAC address and IP address combination for devices and user and passwords for users	Digital signature	The digital signature may be more secure but it's also pricier.
Encryption	Light cryptography techniques like OSGP-AES protocol	Application layer encryption in addition to TLS	Application layer encryption in addition to TLS suggested in [6] has more overhead than our recommended method.
Securing infrastructure	Fiber communication technologies. Separating the smart-meter network from the Internet and other shared internal networks	Gateway-based approach	The gateway is responsible for ensuring the privacy of the customer in [6]. We suggested a more secure infrastructure.
Intrusion Detection	Using IDS and IPS at the edge of the core network	Using IDS and IPS	Similar

[Downloaded from journal.itrc.ac.ir on 2024-05-16]

[DOI: 10.61186/itrc.15.4.32]

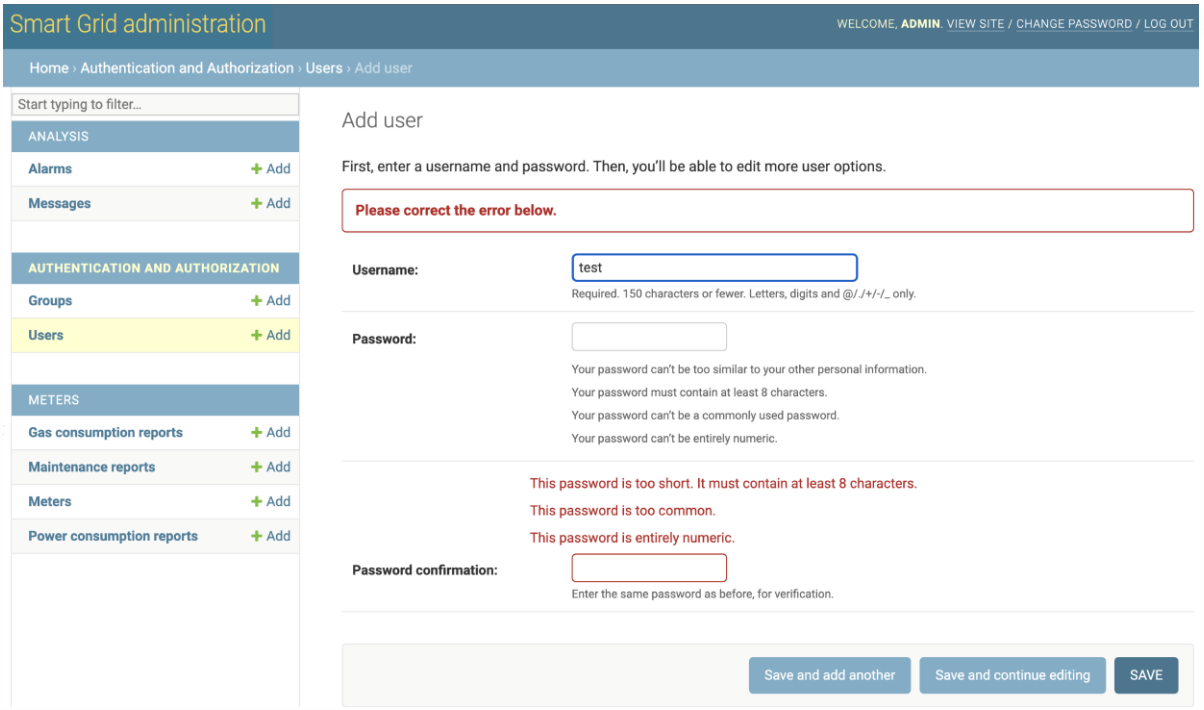

Fig. 1. Password restrictions

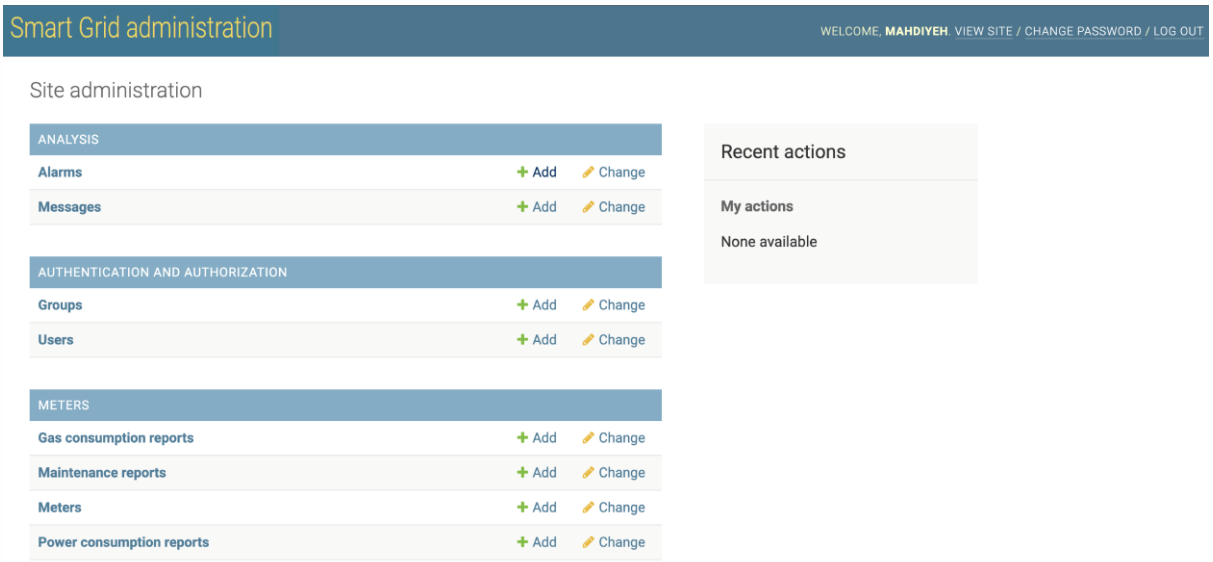

Fig. 2. First page for user from administrators group

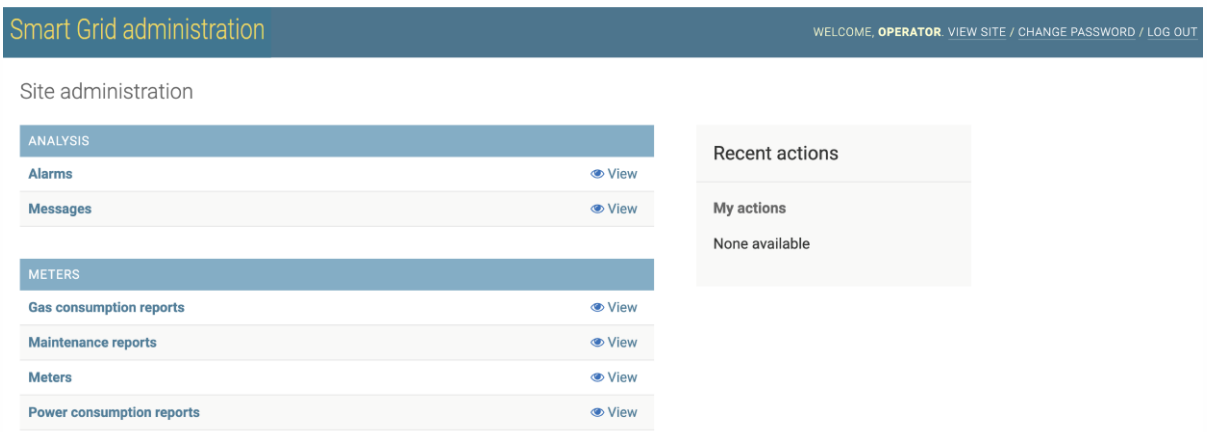

Fig. 3. First page for user from operators group

[Downloaded from journal.itrc.ac.ir on 2024-05-16]

[DOI: 10.61186/itrc.15.4.32]

Fig. 4. Hashed password stored in database table

TABLE IV. ADVANTAGES AND DISADVANTAGES OF THE IMPLEMENTED SECURITY SOLUTIONS

Security Solution	Advantages	Disadvantages
User authentication and defining different levels of access	• No unrestricted access to data • Easier to assign new access or remove it from groups to do it manually for each user • Can assign multiple access groups to users	• Requires extra work at the beginning to define different access groups and determine which group the user belongs to.
Database security	• Hashed password with salt is almost irreversible, even if the attacker gains access to our database.	• Hashed password takes more space in database than a plaintext password.
Securing software infrastructure	• Our website will only be available on our suggested domains and IPs • HTTPS is more secure because of TLS • By disabling DEBUG, the attacker won't be able to use its data.	• TLS has overhead and it will take longer to access our site • We will also be unable to use DEBUG data for debugging issues.
Security against common web attacks	• Prevent Clickjacking attack • Prevent CSRF attack	• Because we disabled framing other websites on our page, we won't be able to use this feature for advertisement purposes either.

REFERENCES

[1] C. C. Sobin, "A Survey on Architecture, Protocols and Challenges in IoT", Wireless Pers Commun 112, 1383–1429 (2020). https://doi.org/10.1007/s11277-020-07108-5.

[2] S. Vashi, J. Ram, J. Modi, S. Verma and C. Prakash, "Internet of Things (IoT): A vision, architectural elements, and security issues," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2017, pp. 492-496, doi: 10.1109/I-SMAC.2017.8058399.

[3] G. Choudhary and A. K. Jain, "Internet of Things: A survey on architecture, technologies, protocols and challenges," 2016 International Conference on Recent Advances and Innovations in Engineering (ICRAIE), 2016, pp. 1-8, doi: 10.1109/ICRAIE.2016.7939537.

[4] Y. Yan, Y. Qian, H. Sharif and D. Tipper, "A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges," in IEEE Communications Surveys & Tutorials, vol. 15, no. 1, pp. 5-20, First Quarter 2013, doi: 10.1109/SURV.2012.021312.00034.

[5] S. Janardhana and M. S. Deekshit Shashikala, "Challenges of smart meter systems," 2016 International Conference on Electrical, Electronics, Communication, Computer and Optimization Techniques (ICEECCOT), 2016, pp. 78-82, doi: 10.1109/ICEECCOT.2016.7955189.

[6] O. Ur-Rehman, N. Zivic and C. Ruland, "Security issues in smart metering systems," 2015 IEEE International Conference on Smart Energy Grid Engineering (SEGE), 2015, pp. 1-7, doi: 10.1109/SEGE.2015.7324615.

[7] F. Farahani and F. Rezaei, "Implementing a Scalable Data Management System for Collected Data by Smart Meters," 2021 26th International Computer Conference, Computer Society of Iran (CSICC), 2021, pp. 1-5, doi: 10.1109/CSICC52343.2021.9420619.

[8] X. Li, X. Liang, R. Lu, X. Shen, X. Lin and H. Zhu, "Securing smart grid: cyber attacks, countermeasures, and challenges," IEEE Communications Magazine, vol. 50, no. 8, pp. 38-45, August 2012, doi: 10.1109/MCOM.2012.6257525.

[9] B. Herzberg, D. Bekerman, and I. Zifman, "Breaking down mirai: An iot ddos botnet analysis," https://www.incapsula.com/blog/malware- analysis-mirai-ddos-botnet.html, october, 2016.

[10] Fortinet. 2021. What is the CIA Triad and Why is it important? [online] Available at: <https://www.fortinet.com/resources/cyberglossary/cia-triad> [Accessed 11 December 2021].

[11] K. Lounis and M. Zulkernine, "Attacks and Defenses in Short-Range Wireless Technologies for IoT," IEEE Access, vol. 8, pp. 88892-88932, 2020, doi: 10.1109/ACCESS.2020.2993553.

[12] N. Mishra and S. Pandya, "Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review," IEEE Access, vol. 9, pp. 59353-59377, 2021, doi: 10.1109/ACCESS.2021.3073408.

[13] O. Ur-Rehman and N. Zivic, "Secure Design Patterns for Security in Smart Metering Systems," 2015 IEEE European Modelling Symposium (EMS), 2015, pp. 278-283, doi: 10.1109/EMS.2015.49.

[14] Kaspersky (2019). What Is a Replay Attack? [online] Available at: https://www.kaspersky.com/resource-center/definitions/replay-attack [Accessed 3 Feb. 2022].

[15] W. Wang and Z. Lu, "Cyber security in the Smart Grid: Survey and challenges", Computer Networks, 57, 1344–1371. 10.1016/j.comnet.2012.12.017.

[16] F. Aloul, A. R. Al-Ali, R. Al-Dalky, M. Al-Mardini, and W. El-Hajj, "Smart Grid Security: Threats, Vulnerabilities and Solutions," International Journal of Smart Grid and Clean Energy, 1, 1-6. 10.12720/sgce.1.1.1-6.

[Downloaded from journal.itrc.ac.ir on 2024-05-16]

[DOI: 10.61186/itrc.15.4.32]

[17] Y. Lee, E. Hwang and J. Choi, "A Unified Approach for Compression and Authentication of Smart Meter Reading in AMI," IEEE Access, vol. 7, pp. 34383-34394, 2019, doi: 10.1109/ACCESS.2019.2903574.

[18] Security guide for Industrial Protocols Smart Grid. (n.d.). [online] Available at: https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/incibe-cert_guide_protocols_smart_grid_2017_v2.pdf.

[19] Django, L. (n.d.). Django Best Practices: Security. [online] learndjango.com. Available at: https://learndjango.com/tutorials/django-best-practices-security [Accessed 8 Feb. 2022].

[20] Hamza Khan (2014). What is SSL? - SSL.com. [online] Available at: https://www.ssl.com/faqs/faq-what-is-ssl/.

Mahdiyehsadat Mirsharifi received her B.Sc. in Computer Engineering from K. N. Toosi University of Technology, Tehran, in 2022, and now she is pursuing her M.Sc. degree in Communication Systems and Networks at Tampere University. Her research interests include Computer Networks, Cloud Computing, and Cyber Security. She also uses these research results daily as a DevOps Engineer.

Fatemeh Rezaei received the B.Sc., M.Sc., and Ph.D. degrees in Electrical Engineering from the Sharif University of Technology, Tehran, Iran, in 2010, 2012, and 2017, respectively. In 2015, she spent a sabbatical stay with KTH University, Stockholm, Sweden. She is currently an Assistant Professor with the Department of Computer Engineering, K. N. Toosi University of Technology, Tehran, Iran. Her current research interests include Wireless Networks and Edge Computing.

[Downloaded from journal.itrc.ac.ir on 2024-05-16]

[DOI: 10.61186/itrc.15.4.32]