Identity and Access Management for IoT in Smart Grid

Vilmar Abreu, Altair O. Santin, Eduardo K. Viegas and Vinicius V. Cogo

Abstract A smart grid (SG) is a complex system that comprises distributed servers and Internet-of-Things (IoT) devices. IoT devices are resource-constrained and are unable to cope with traditional communication and security protocols. In light of this limitation, this work proposes a novel method for end-to-end secure communication between the elements in the SG. Our proposal enables an authenticated user to transport her Internet credentials to the IoT context. We provide high efficiency in the message exchanges by adopting multicast communication without compromising the SG security. However, even though this process provides secure communication, it cannot enforce fine-grained access control over protected resources. Therefore, we propose a new two-step lightweight access control mechanism that leverages the established configuration to provide role-based authorization in the IoT context. The prototype evaluation shows that our proposal is more flexible, demanding less manual configuration, while also requires only 23% of message exchanges compared to other approaches in the literature.

1 Introduction

Smart Grids (SG) are complex systems controlled by electric energy systems to act integrated through computational intelligence and network communication for gen-

Vilmar Abreu
Pontifical Catholic University of Parana, Brazil (PUCPR), e-mail: vilmar.abreu@ppgia.pucpr.br

Altair O. Santin
Pontifical Catholic University of Parana, Brazil (PUCPR), e-mail: santin@ppgia.pucpr.br

Eduardo K. Viegas
Pontifical Catholic University of Parana, Brazil (PUCPR), e-mail: eduardo.viegas@ppgia.pucpr.br

Vinicius V. Cogo
LASIGE, Faculdade de Ciências, Universidade de Lisboa, Portugal e-mail: vvcogo@fc.ul.pt

eration, transmission, distribution, measuring, and billing energy consumption [11]. An SG is responsible for the control and supervision of critical infrastructures [20]. Critical infrastructures are composed of (virtual or physical) systems and assets that are vital for a nation. Thus, their unavailability or destruction may have a high impact on the security and economic aspects of a country.

Over the last years, many authors have shown that energy systems are vulnerable to cyberattacks [6]. A common vulnerability root-cause is related to the substitution of traditional Power Line Controllers (PLC) for embedded systems, and Internet-of-Things (IoT) devices, which can be remotely controlled through the Internet [22]. However, using such processing and sensing devices is a natural trend in Industry 4.0. As a result, devices being exposed on the Internet renders vulnerable the whole critical infrastructure [19].

Due to several recent cyberattacks, government agencies have shown great concern in SG cybersecurity. For instance, in 2010, an electric power plant suffered a cyberattack that caused over 900 Megawatt losses in less than 7 seconds [5]. Later, in the same year, an Iranian nuclear power plant was attacked by Stuxnet [15], causing severe physical damages [21]. According to a CIA report, several energy systems were invaded by hackers in the USA, causing even cities blackouts [5].

Consequently, several widely recognized entities—e.g., IEC (*International Electrotechnical Commission*), NERC (*North American Electric Reliability Corporation*), and IEEE (*Institute of Electrical and Electronics Engineers*)—have defined a set of SG standardized security requirements to protect electric energy systems, and more specifically SGs. However, these security requirements are too coarse-grained. Additionally, IEC [9] has shown that these standards do not cope with the complexity of SG architectures, neither with the ubiquitous nature of IoT devices.

The security of IoT devices (e.g., smart meters) is essential for the SG, where compromising a device puts the whole infrastructure at risk [2]. The main challenge in ensuring IoT security is in their computational constraints, which renders the usage of traditional security mechanisms and communication protocols unfeasible [28]. As a result, it creates a technological and interoperability gap for the deployment of traditional Identity and Access Management (IAM) mechanisms.

In light of this limitation, our work enables IAM authenticated users to transport their credentials to the IoT context while ensuring communication authenticity and confidentiality. We propose a disposable password approach (i.e., One Time Password—OTP) to perform secure (unicast or multicast) communication between the IoT and Internet entities. However, despite our approach being able to provide end-to-end secure communication, it is unable to provide fine-grained access control over the IoT protected resources. Therefore, our proposed IAM relies upon a lightweight access control, suited for resource-constrained IoT devices, to control the user access to protected IoT resources. As a result, the main contributions of this paper are as follows:

- An end-to-end OTP-based secure communication between the Internet and IoT devices. It uses multicast protocol suited for the resource-constrained IoT devices. It significantly decreases the number of exchanged messages required to query information from smart-meters with authenticity and confidentiality;

- A dynamic, secure scheme for the definition of IoT symmetric key used in the Datagram Transport Layer Security (DTLS). It dynamically builds and shares the secret keys required for secure communication between distributed entities;
- A lightweight role-based access control for IoT environments. It provides fine-grained access control while also sharing and updating the used passwords (keys) among the IoT devices;

2 Related Works

Over the last years, numerous works have proposed enhanced security for IoT devices [27]. Beyond context-specific functionalities, an IoT device typically can inform its manufacturer of the occurrence of technical issues. As a result, the manufacturer may remotely access the device to repair or update its firmware. In such a case, remotely accessing thousands of devices is a common requirement, which requires individual authentication in each device. Consequently, to address such a case, related works typically isolate the devices for security reasons [29]. Additionally, these works generally restrict the device's communication and access. Authentication and authorization are well-known challenges in the IoT context. Due to the constrained computational power of such devices, using traditional security mechanisms is impractical [26]. As a result, finding in the market solutions that rely on a single default password or unique key for the device access is common [25]. Although this approach provides low resource consumption, discovering the single key or password compromises all devices with the same configuration [14, 17, 30]. Additionally, updating the key or password in all devices is challenging and have been explored by several related works.

For instance, Liu *et al.* [16] proposed a solution for authentication and access control for IoT. Their work employs the OpenID and Role-based Access Control (RBAC) in the IoT context. Although their work applies well-known security mechanisms, porting such techniques to the IoT context is not addressed. Additionally, communication confidentiality or SSO (Single Sign-On) are also not provided. In contrast, Ammayappan *et al.* [3] proposes an SG authentication protocol based on both symmetric and asymmetric cryptography to ensure communication authentication and confidentiality. Although they provide a lightweight mechanism, they rely on asymmetric keys, which is not recommended for the IoT context, due to a high computational resource requirement [1]. In Chin *et al.* [8], a Machine-to-Machine (M2M) authentication platform was proposed for SG. Their proposal is based on digital signatures, in which a concentrator entity enables the key sharing between the contexts. However, it creates a single point of failure, besides applying the public key cryptography in IoT context. The work of Chavan *et al.* [7] noted that the HTTP protocol is inefficient for the computational constraints of IoT devices. The authors applied the Constrained Application Protocol (CoAP) coped with DTLS, to ensure communication confidentiality. However, they combined these protocols with a public key mechanism.

Hou *et al.* [13] have mathematically shown the security importance of the SSO in the IoT device authentication. Garcia *et al.* [12] have performed a series of security analysis in the DTLS protocol and they evidenced well-known vulnerabilities, such as those present in the TLS protocol. Thus, to mitigate such vulnerabilities, Shiivraj *et al.* [24] have proposed a two-factor authentication mechanism based on OTP. They coped the Lamport algorithm with elliptic curves to ensure the end-to-end authentication in IoT. Their prototype is computationally efficient when deployed in an Android smartphone. However, they did not evaluate the performance of their work in constrained devices (e.g., with limited processing or memory, battery-powered, or with limited network bandwidth). Witkovski *et al.* [29] proposed a cryptography-based authentication mechanism for IoT, which leverages SSO. Their work is based on ANSI X.9.17 [18], in which two hierarchical levels of symmetric keys are used to perform the communication between the Internet and the IoT devices. Finally, Shanta *et al.* [4] systematically reviewed IoT authentication techniques. They have concluded that the authentication and data protection mechanisms for the IoT context must be lightweight while not compromising the system security.

3 Proposal

3.1 A Disposable Password Approach for End-to-End Security

Our proposal takes into account the resource-constrained nature of IoT, which inhibits the usage of traditional Internet security mechanisms, such as the TLS. It relies on two cryptographic levels to ensure end-to-end communication security. First, our proposal applies, at the external level, a symmetric key for the IoT entities (DTLS) and public-key cryptography for the Internet entities (TLS). Second, at the internal level, the symmetric key cryptography is applied, which demands less processing than the public key cryptography.

Our proposal relies on the disposable password concept (e.g., OTP) to mitigate a possible breach of the symmetric key used at the internal level. The disposable password is used as a symmetric key to encrypt the communication between the Internet and the IoT entities. Therefore, we apply the Time-based One Time Password (TOTP) to perform the end-to-end communication between the CS and SM according to the Hashed Message Authentication Code (HMAC).

As a result, each SM holds a symmetric key shared with the central system (CS), as shown in Figure 1. The symmetric key employs the concept of master key, namely Local Master Key (LMK), which is never transferred in the network. Therefore, it must be stored at the SM manufacturer production line protected by hardware, e.g., smart card. In the CS, the LMK is stored in a secure key database, such as the Kerberos Key Distribution Center (KDC).

The generated TOTP value also relies upon a proper dynamic incremental counter, which is shared between the IoT and Internet entities. The counter is shared

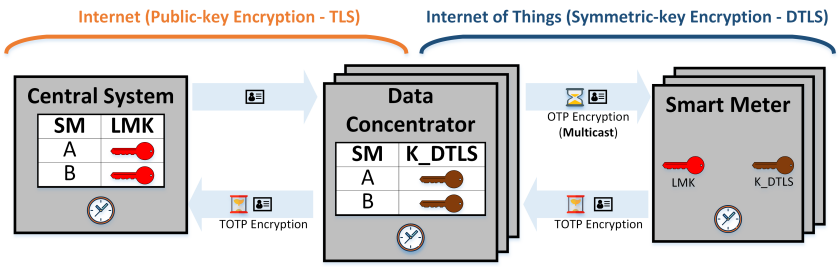


Fig. 1: Proposed disposable password for end-to-end security.

between the CS and the smart-meter (SM) to ensure end-to-end communication, and another counter is shared between the data concentrator (DC) and SM to protect the multicast communication. The goal of multicast communication is to decrease the number of exchanged messages, considering that a CS usually requests data stored in several SMs. Consequently, the shared disposable key created by the TOTP is used as a communication group key.

All parameters but LMK (e.g., DTLS keys and counters) are dynamically and securely established through the network, as shown in Figure 1. The DC builds a new K_DTLS and ciphers it with the CS public key. Then, it forwards the request for the CS to cipher the K_DTLS with the LMK. The CS deciphers the message using the private key to cipher it in the LMK. The DC receives the ciphered message with its public key and deciphers it with its private key. Finally, the DC forwards the ciphered K_DTLS to the SM, which will be deciphered in the SM LMK. This process is also used to establish the DC and SM counters.

The whole communication is ciphered, whereas the public key cryptography protects the communication between the CS and DC. The communication between the CS and SM is protected by the symmetric key cryptography, in which the LMK is never exposed or transmitted in the network.

The multicast communication employed between the DC and SM relies on the traditional OTP method instead of using the TOTP. The OTP method does not employ a cryptographic key (LMK) to build a disposable password, which brings two main benefits. First, it prevents the need for sharing a cryptographic key between the DC and SM. Second, the request messages usually do not contain sensitive data. We only apply two-layer cryptography on responses. The internal layer is ciphered using the password (key) created by the TOTP, while the DC can only decipher the external layer, i.e., it is not a single point of failure (Figure 2).

After this initial configuration, it is possible to apply the end-to-end security protocol employing the OTP approach. An IAM authenticated operator performs a request, through the CS, for instance, of the energy consumption of all SMs in a specific region, supplying her access token. Then, the DC validates the access token in the IAM, and if it is valid, it builds a new key through the OTP to be used as a group key. Thus, the CS request is ciphered in the group key and transmitted for all SMs through multicast. Hence, all SMs multicast members receive the ciphered message

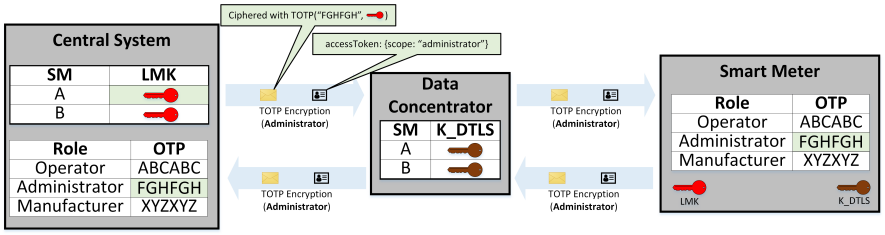


Fig. 2: Example scenario of an administrator accessing the IoT context.

and use the generated OTP to decipher the request. Therefore, after processing the CS request, the SM builds a key using the TOTP, parameterized by the LMK. This key is then used to cipher the response which will be sent for the DC, ciphered in the K_DTLS.

It is important to note that this process ensures end-to-end communication security, taking into account that the whole communication is ciphered. In such a context, the DC reads the content of the CS request messages sent to the SMs. However, the DC cannot read the SMs responses, assuming that they are ciphered using the key build by the TOTP, which applies the LMK shared between the CS and SM. A possible alternative of such a process is to allow the DC to act as a data aggregator. In such a case, the SM responses would be ciphered only with the K_DTLS, instead of the TOTP. Thus, the DC deciphers the message content, to aggregate and summarize the information before sending the data to the CS, decreasing processing demand.

3.2 Lightweight Access Control

Although the proposed approach provides end-to-end communication security between the IoT devices, the access control for the IoT remains an open challenge. This because the provided access token authorization control restricts the access to a protected resource, but does not support the establishment of policies to define the allowed operations over the resources. As a consequence, it is not possible to provide fine-grained access control over protected resources.

The traditional access control architecture is typically composed of a reference monitor, an authorization database, and a mechanism keeper [23]. However, this architecture is not suited for the IoT resource-constrained nature. Therefore, we propose a lightweight access control mechanism in both processing, transmission, and memory needs based on symmetric keys. Our mechanism leverages the established configuration (shown in Section 3.1) to provide role-based access control in which the user has access rights according to her organization's role. Additionally, our mechanism does not employ the session concept defined in the RBAC model [23], which simplifies the implementation and deployment of our scheme in IoT devices.

For instance, to access an SM, three roles can be defined: operator, administrator, and manufacturer, as shown in Figure 2. The first role, the operator, can perform

queries, such as reading operations, on top of protected resources. In contrast, the administrator can perform writing requests for device parameterization purposes over protected resources. Finally, the manufacturer can perform both reading and writing requests over the SMs, which includes firmware updates, for instance.

It is important to note that other roles can be defined. However, for the sake of simplicity, we consider a scenario of only three primary roles. Thus, each role holds an associated dynamic TOTP counter in both CS and SM, as shown in Figure 2. When a specific administrator desires to access an SM, she must cipher the request using her disposable password, built by the associated TOTP. In such a case, the TOTP uses a dynamic administrator counter with the LMK of a specific SM to build a proper disposable password, which is then used as a symmetric key.

As a consequence, when the SM receives the request, it will attempt to decipher it using the associated counter with each defined role, starting with the operator, then the administrator and finally the manufacturer. However, for instance, this role sequence could be ordered by the operation frequency for each role. To ensure that the SM can decipher the message, the CS forwards both the deciphered request identifier and the TOTP ciphered request identifier. If the deciphered identifier is equal to the received identifier, the used counter is correct, and the SM can infer the associated role.

Therefore, our proposed access control ensures that the user has access control authorization in a twofold manner. First, she must have an access token with the proper request scope. Second, she must be able to decipher the SM response, which is ciphered in with the LMK and the role counter. Compromising the SM requires an attacker to have access to both the access token and the role counter.

4 Prototype

The prototype was developed through well-known standards, consolidated technologies, and open-source libraries. The IAM implementation used the identity and access management server WSO2 Identity Server as its base platform, which enables the usage of several protocols, such as the OpenID, OpenID Connect, SAML, Passive STS among others. To perform the authentication, the OpenID Connect Protocol was configured as IdP at the WSO2. The OAuth 2.0 protocol, used in the OpenID Connect is responsible for the access authorization, issuing access tokens through the JWT format (JSON Web Token).

Figure 3 shows the proposed architecture, including the used protocol stack in each entity to ensure secure communication. At the Internet perspective, the HTTPS protocol is used. In contrast, at the IoT perspective, the CoAP with DTLS is used. The CoAP protocol is based on the REST architecture, where each resource is accessed through a URL. The CoAP uses the UDP at the transport layer, which is a protocol suited for resource-constrained devices.

The DC was implemented in Java, while an HTTP server was used for providing its Internet interface. For the IoT interface, the CoAP was used through the Cali-

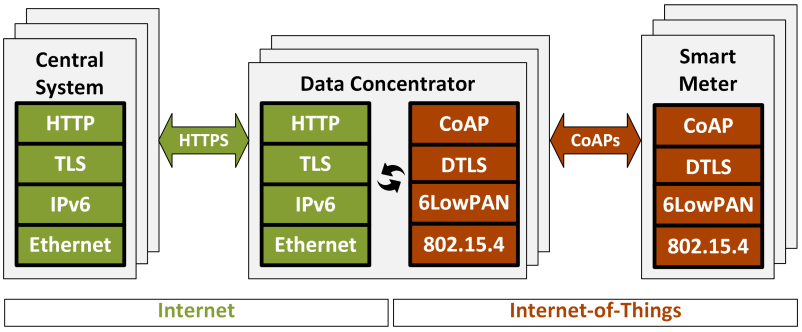


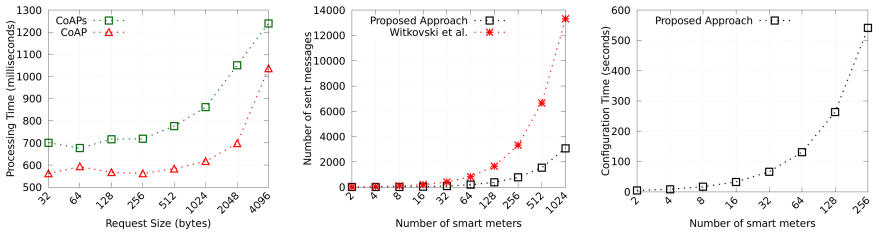
Fig. 3: Prototype implementation protocol stack.

fornium library. Consequently, the DC can forward messages between HTTP and CoAP, and vice-versa. The SM was developed in Java, also using the Californium library and executed in ContikiOS [10]. The AES algorithm with 128 bits key size was used to encrypt messages. For the DTLS, the prototype relies upon the Scandium library version 1.2, which is a Californium sub-project. To perform the disposable password generation, the AeroGear library was used, while the REST services were provided through Jersey.

5 Evaluation

The proposal evaluation was performed in a controlled environment, hence, decreasing external interference. In total, four machines were used, all interconnected through a Gigabit network. Each machine has an Intel Core i7 CPU and 8GB of memory. One machine was used to host the IAM, while another was used to execute the Contiki OS. As stated in Section 4, our proposal used the DTLS to ensure the security of the IoT devices communications. Therefore, our first evaluation comprises the processing time impact when the CoAPs is used. To this end, we vary the message request size sent to the SM.

Figure 4a shows the processing time comparison between CoAP and CoAPs (CoAP with DTLS). Additionally, it is possible to note that the processing time increases according to the request size. However, such processing time increase is not proportional, hence, being advantageous at the security perspective. But, the processing time impact (170ms) does not degrade the SG performance, as it is, in general, made of thousands of SMs, which are queried in parallel, through our proposed multicast scheme.



(a) (b) (c)

Fig. 4: (a) CoAP and CoAPs processing time comparison. (b) End-to-end communication processing time comparison according to the number of used smart meters. (c) OTP-based initial configuration time.

5.1 Scalability

To evaluate our proposed OTP-based end-to-end security, we have compared it with the Witkovski [29] proposal. Their technique applies the concept of hierarchical keys in an uncoupled and asynchronous manner. Hence, the CS is not able to inject information directly to the SM, it is only able to deposit it in the DC. Such an approach mitigates the possibility of an adversary to inject malicious code or control an SM, considering that she does not have an interactive session.

In their approach, to establish the communication [29], the SM periodically queries the DC, verifying whether there are pendent queries or not. Similarly, after the CS performs a request to the DC, it queries the response to its query through the ticket concept. Therefore, this decoupling between entities significantly increases the number of exchanged messages, due to the performed pooling. This characteristic is worsened in the IoT context, due to the constrained processing nature of devices. Additionally, for the CS and SM to obtain a proper key, several messages are needed. Thus, in a scenario in which the number of SM is high, the situation worsens, considering that the communication is unicast.

The Witkovski [29] approach is close to ours, however, our proposed scheme decreases the number of messages by leveraging the multicast communication. Our OTP-based approach has some main advantages over the them. We decrease the number of exchanged messages by multicasting between CS and SMs. It is important to note that our approach maintains communication security by applying group cryptography in multicast queries. Additionally, the queries responses are encrypted end-to-end with the TOTP generated keys. Considering that the cryptography key (OTP) used in the request is weaker than the cryptographic key (TOTP) used in the response, considering that it holds sensitive data. Furthermore, the OTP-based approach enables the K_DTLS key to easily updated, while in the Witkovski [29] approach, the K_DTLS must be manually defined. Finally, our OTP-based approach enhances the process flexibility, considering that it enables the DC to act as the gateway or data aggregator.

Table 1: End-to-End communication comparison of the number of sent messages.

Characteristics	Witkovski[29]	Our Approach
Total Number of Messages	$N * 13$	$6 + (N*3)$
Symetric Cryptography in IoT	$N * 4$	$N * 4$
Hash Function in IoT	0	N
Key Generation in IoT	$N * 2$	$N * 3$
Counter Sharing	0	$N * 2$

Table 1 shows the number of exchanged between both approaches, in which N denotes the number of SMs in the scenario. In the table, we consider the process of an CS requesting a data to an SM, and its proper reply to the CS. It is possible to note that our technique significantly decreases the number of exchanged messages. For instance, in a 256 SMs scenario, our approach demands only 774 messages to be sent, while in Witkovski [29] proposal, 3328 messages are sent (increase of 329%). It is important to note that a typical SG environment can be made of millions of SMs. Therefore, our approach, which demands fewer messages to be exchanged presents an important benefit, specially for IoT environments.

Figure 4b shows a comparison between the number of exchanged messages according to the number of Smart Meters. The relation between the processing demand (e.g., number of ciphering, key generation, and hash functions) is similar between both approaches, while their main difference occurs when the number of SMs is high. In a scenario with more than 128 SMs, for instance, the proposal from Witkovski [29] is not easily scalable. Although a typical SG architecture is made of millions of SMs, each DC holds only a subset of SMs. However, the decrease in the number of exchanged messages is of high interest in such environments, at the same time, it maintains the communication security.

5.2 The Initial Configuration Cost

Finally, we evaluate the configuration time of our approach. This because, as our OTP-based scheme demands further parameters to be set dynamically set between the entities, such as secure distribution of the DTLS key. As a consequence, our technique increases the time needed before secure communication is established.

Figure 4c shows the configuration time according to the number of used smart meters. It is possible to note that our proposed approach configuration time increases according to the number of SMs in the environment. However, this configuration time is only demanded at the initial system deployment. Over time, when new SMs are added to the CS controlled environment, the configuration time remains low, as only a subset of SMs must be configured. Therefore, our proposed scheme dynamically and securely exchanges messages between the Internet and IoT entities. This because, we demand fewer messages to be exchanged, hence, supporting further

SMs, while also provides a low configuration time, considering that new SMs can be added over time, with low processing impact over the whole architecture.

6 Conclusions

The SG provides several benefits for society by means of applying intelligence computing and communication technologies in an integrated manner. However, those benefits imply cyber security challenges, which demand mechanisms more efficient in securing the SG against cyberattacks. Surprisingly, the literature lacks cyber security mechanisms adequate for the SG characteristics. Therefore, in this work, we have proposed an OTP-based secure multicast for IoT context suited for the resource-constrained nature of IoT devices. Our proposed approach enables establishing the DTLS key in a dynamic and secure manner. Additionally, we have proposed a lightweight role-based access control for IoT, which enables fine-grained control over protected resources. Our proposed end-to-end OTP-based scheme presents as its main benefit the efficient message exchange, by applying the multicast communication without compromising the system security. The proposal evaluation has shown that our proposed scheme improves the state-of-the-art techniques, while also presenting more flexibility over the parameter setting.

Acknowledgments

Authors thank CNPq (Conselho Nacional de Desenvolvimento Científico e Tecnológico) for partial financial support (grant 430972/2018-0 and 315322/2018-7) and the FCT through the LASIGE Research Unit (ref. UIDB/00408/2020).

References

1. Abreu, V., Santin, A., Xavier, A., Lando, A., Witkovski, A., Ribeiro, R., Stihler, M., Zambenedetti, V., Chueiri, I.: A smart meter and smart house integrated to an idm and key-based scheme for providing integral security for a smart grid ict. Mobile Networks and Applications **23**(4), 967–981 (2018)
2. Abreu, V., Santin, A.O., Viegas, E.K., Stihler, M.: A multi-domain role activation model. In: 2017 IEEE International Conference on Communications (ICC). IEEE (2017)
3. Ammayappan, K., Saxena, A., Negi, A.: Mutual authentication and key agreement based on elliptic curve cryptography for gsm. In: 2006 International Conference on Advanced Computing and Communications, pp. 183–186 (2006)
4. Arockiam, L., Joshitta, R.S.: Authentication in iot environment: A survey. nternational Journal of Advanced Research in Computer Science and Software Engineering **6**, 140–145 (2016)
5. Ashibani, Y., Mahmoud, Q.H.: Cyber physical systems security: Analysis, challenges and solutions. Computers & Security **68**, 81 – 97 (2017)

6. Cárdenas, A.A., Amin, S., Sastry, S.: Research challenges for the security of control systems. In: Proceedings of the 3rd Conference on Hot Topics in Security, HOTSEC'08, pp. 6:1–6:6. USENIX Association, Berkeley, CA, USA (2008)
7. Chavan, A.A., Nighot, M.K.: Secure and cost-effective application layer protocol with authentication interoperability for IOT. Procedia Computer Science **78**, 646–651 (2016)
8. Chin, W., Lin, Y., Chen, H.: A framework of machine-to-machine authentication in smart grid: A two-layer approach. IEEE Communications Magazine **54**(12), 102–107 (2016)
9. Commission, I.E.: Iec smart grid standardization roadmap (2010). URL https://www.iec.ch/smartgrid/downloads/sg3_roadmap.pdf
10. Contiki: Contiki os (2019). URL https://www.contiki-ng.org/
11. Fang, X., Misra, S., Xue, G., Yang, D.: Smart grid — the new and improved power grid: A survey. IEEE Communications Surveys Tutorials **14**(4), 944–980 (2012)
12. Garcia-M., O., Keoh, S.L., Kumar, S., M., P., Vidal-M., F., Z., J.H.: Securing the ip-based internet of things with hip and dtls. In: ACM Conference on Security and Privacy in Wireless and Mobile Networks, WiSec '13, pp. 119–124. ACM, New York, NY, USA (2013)
13. Hou, J.L., Yeh, K.H.: Novel authentication schemes for iot based healthcare systems. Int. J. Distrib. Sen. Netw. **2015**, 5:5–5:5 (2016)
14. Infoworld: Millions of embedded devices use the same hard-coded ssh and tls private keys (2015). URL http://www.infoworld.com/article/3009667/security/millions-ofembedded-devices-use-the-same-hard-coded-ssh-and-tls-privatekeys.html
15. Langner, R.: Stuxnet: Dissecting a cyberwarfare weapon. IEEE Sec. & Priv. **9**, 49–51 (2011)
16. Liu, J., Xiao, Y., Chen, C.L.P.: Authentication and access control in the internet of things. In: 2012 32nd International Conference on Distributed Computing Systems Workshops, pp. 588–592 (2012). DOI 10.1109/ICDCSW.2012.23
17. News, H.: Millions of iot devices using same hard-coded crypto keys (2015). URL http://thehackernews.com/2015/11/iot-devicecrypto-keys.html
18. NIST: Ansi x9.17 key distribution (1992). URL https://www.niatec.iri.isu.edu/(S(5pvzas455hrdzsrxbwh1ndqb))/GetFile.aspx?pid=60
19. NIST: Framework for cps cybersecurity (2018). URL https://nvlpubs.nist.gov/nistpubs/
20. NIST: Iam for electric utilities (2018). URL https://nvlpubs.nist.gov/nistpubs/
21. Peng, Y., Lu, T., Liu, J., Gao, Y., Guo, X., Xie, F.: Cyber-physical system risk assessment. In: Int. Conf. on Intelligent Inf. Hiding and Mult. Signal Processing, pp. 442–447 (2013)
22. Ribeiro, R., Santin, A., Abreu, V., Marynowski, J., Viegas, E.: Providing security and privacy in smart house through mobile cloud computing. In: 2016 8th IEEE Latin-American Conference on Communications (LATINCOM). IEEE (2016)
23. Sandhu, R.S., Coyne, E.J., Feinstein, H.L., Youman, C.E.: Role-based access control models. Computer **29**(2), 38–47 (1996)
24. Shivraj, V.L., Rajan, M.A., Singh, M., Balamuralidhar, P.: One time password authentication scheme based on elliptic curves for internet of things (iot). In: 2015 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW), pp. 1–6 (2015)
25. Vicentini, C., Santin, A., Viegas, E., Abreu, V.: SDN-based and multitenant-aware resource provisioning mechanism for cloud-based big data streaming. Journal of Network and Computer Applications **126**, 133–149 (2019)
26. Viegas, E., Santin, A., Abreu, V., Oliveira, L.S.: Enabling anomaly-based intrusion detection through model generalization. In: 2018 IEEE Symposium on Computers and Communications (ISCC). IEEE (2018)
27. Viegas, E., Santin, A., Oliveira, L., França, A., Jasinski, R., Pedroni, V.: A reliable and energy-efficient classifier combination scheme for intrusion detection in embedded systems. Computers & Security **78**, 16–32 (2018)
28. Viegas, E., Santin, A.O., Franca, A., Jasinski, R., Pedroni, V.A., Oliveira, L.S.: Towards an energy-efficient anomaly-based intrusion detection engine for embedded systems. IEEE Transactions on Computers **66**(1), 163–177 (2017)
29. Witkovski, A., Santin, A., Abreu, V., Marynowski, J.: An idm and key-based authentication method for providing single sign-on in iot. In: IEEE GLOBECOM, pp. 1–6 (2015)
30. ZDnet: Smart meter hacking tool released (2012). URL http://www.zdnet.com/article/smart-meter-hacking-tool-released