sustainability

MDPI

Article

Digital Certificate Verification Scheme for Smart Grid using Fog Computing (FONICA)

Shahid Mahmood [1], Moneeb Gohar [1,*], Jin-Ghoo Choi [2], Seok-Joo Koh [3,*], Hani Alquhayz [4] and Murad Khan [3]

[1] Department of Computer Science, Bahria University, Islamabad 44000, Pakistan; 01-247181-024@student.bahria.edu.pk
[2] Department of Information and Communication Engineering, Yeungnam University, Gyongsan 38541, Korea; jchoi@yu.ac.kr
[3] School of Computer Science and Engineering, Kyungpook National University, Daegu 41566, Korea; mkhan@knu.ac.kr
[4] Department of Computer Science and Information, College of Science in Zulfi, Majmaah University, Al-Majmaah 11952, Saudi Arabia; h.alquhayz@mu.edu.sa
* Correspondence: mgohar.buic@bahria.edu.pk (M.G.); sjkoh@knu.ac.kr (S.-J.K.); Tel.: +82-53-950-7356 (S.-J.K.)

Abstract: Smart Grid (SG) infrastructure is an energy network connected with computer networks for communication over the internet and intranets. The revolution of SGs has also introduced new avenues of security threats. Although Digital Certificates provide countermeasures, however, one of the issues that exist, is how to efficiently distribute certificate revocation information among Edge devices. The conventional mechanisms, including certificate revocation list (CRL) and online certificate status protocol (OCSP), are subjected to some limitations in energy efficient environments like SG infrastructure. To address the aforementioned challenges, this paper proposes a scheme incorporating the advantages and strengths of the fog computing. The fog node can be used for this purpose with much better resources closer to the edge. Keeping the resources closer to the edge strengthen the security aspect of smart grid networks. Similarly, a fog node can act as an intermediate Certification Authority (CA) (i.e., Fog Node as an Intermediate Certification Authority (FONICA)). Further, the proposed scheme has reduced storage, communication, processing overhead, and latency for certificate verification at edge devices. Furthermore, the proposed scheme reduces the attack surface, even if the attacker becomes a part of the network.

Keywords: digital certificate revocation; smart grid (SG); Internet of Things; CRL; OCSP; edge devices; fog computing; IoT Devices; FONICA

check for updates

Citation: Mahmood, S.; Gohar, M.; Choi, J.-G.; Koh, S.-J.; Alquhayz, H.; Khan, M. Digital Certificate Verification Scheme for Smart Grid using Fog Computing (FONICA). *Sustainability* **2021**, *13*, 2549. https://doi.org/10.3390/su13052549

Academic Editors: Amir Mosavi and Mohsin Raza

Received: 3 December 2020
Accepted: 16 February 2021
Published: 26 February 2021

1. Introduction

Infrastructure used for asymmetric key cryptography is also known as PKI (Public Key Infrastructure). PKI has resolved many security issues of symmetric key cryptography and out of them, one major issue was non-repudiation. The issue of non-repudiation was resolved by PKI and it was the big reason for its success. Later, a new issue was revealed that the-middle attacks could be launched by forging public key. The concept of PKI infrastructure is based on the accessibility of public key will remain to everyone while private key will be kept secret with the owner. This public key can be used by anyone for encryption and output ciphertext will be decrypted by private key only. Similarly, the private key can also be used for encryption and the public key can be used for decryption. Decryption using a public key verifies that encryption is performed by the owner of the corresponding private key. Therefore, owner cannot repudiate. In this way security service of non-repudiation will be achieved [1]. Due to the public accessibility of the public key, it can be misrepresented by an attacker. Anyone can claim to be the owner of any public key; therefore, centralized authority is required for binding the public key with an identity. The centralized authority is called CA (Certification Authority).

Digital Certificates are used for binding a public key with an identity and authenticity trusted by a third party, i.e., CA over the internet. All these requirements are also applicable to Internet of Things (IoT) and Smart Grid (SG) networks [2,3]. Similarly, the edge devices are required to be updated immediately after CA declare a certificate status is revoked [4,5]. Otherwise, attacker may get connected with an edge device, pretend to be a trusted device that may lead to loss of sensitive information. Efficient distribution of information about revoked certificates among edge devices in a SG environment in a resource efficient way is a challenging job. Specifically, SG infrastructure always requires an efficient and reliable communication and computation infrastructure to carry and process the associated data [6]. In this paper, an efficient certificate verification scheme has been proposed which mathematically shows efficient results based on storage and communication overhead parameters as compared to other recently proposed schemes "Bloom Filter". The proposed scheme will eliminate storage requirements from edge devices and the response time required for certificate verification within the trusted area of fog. The scheme is compatible with the existing mechanism being used by international Certification Authorities. Following Table 1 shows list of abbreviations used in rest of the paper.

Table 1. List of Acronyms.

Ser	Abbrivation	Meaning	Ser	Abbrivation	Meaning
1	SG	Smart Grid	2	CIA	Confidentiality, Integrity, and Availability
3	IoT	Internet of Things	4	PKI	Public Key Infrastructure
5	CA	Certification Authority	6	DTLS	Datagram Transport Layer Security
7	CRL	Certification Revocation List	8	IKE	Internet Key Exchange
9	OCSP	Online Certificate Status Protocol	10	TLS	Transport Layer Security
11	BF	Bloom Filter	12	ICT	Information and communications technology
13	SLC	Short-Lived Certificate	14	SSL	Secure Sockets Layer
15	DS	Digital Signatures	16	FONICA	Fog Node acting as intermediate certification Authority
17	IAS	Information Assurance Services	18	ADOPT	Ad-hoc Distributed OCSP for Trust

1.1. Digital Certificates and Certification Authority (CA)

Digital Certificates are used for binding a public key with the identity of an entity using digital signatures [7], trusted by a third party called CA. Digital Certificates include the information of public key, signature algorithm, issuer, expiration date, and so on. These certificates are also the requirement of the SG environment. The edge device which receives the certificate will also verify the certificate. The edge device verifies a chain of trust, verify signatures using the public key of CA, and obtains revocation status. CA is a trusted third party, which may be a government agency or any other financial institution on which consumer and service providers can trust. W3Techs survey has reported that in Dec 2020 top three well-known CA are IdenTrust, DigiCert, and Sectigo. Edge devices are required to verify different certificates by keeping in view the limitations of computational power, storage, battery lifetime, and bandwidth issues.

1.2. Role of Fog Computing in Security of SG

SG infrastructure provides energy efficient services in continuously, reliable and secure fashion. Security is one of most critical element for efficient delivery of services. Security services in real-time can be efficiently achieved using fog computing rather than cloud computing [8,9]. Fog computing is also known as edge computing. Fog computing has three-layer architecture, i.e., client, fog nodes, central server [10,11]. The objective of fog computing is to bring services closer to the edge device. The difference between cloud and fog computing can be represented as (Processing power of Cloud > Processing power of Fog node > Processing power of edge device) and the placement of fog node at the edge of the local network [12,13]. In fog computing, edge nodes can access local data without involving the cloud. Only filtered data will travel to the cloud and this will result in efficient utilization of network bandwidth as well as storage capacity and processing resources of the cloud [14]. Fog nodes capacity may vary from limited resources to high power computational device(s). Generally, the fog layer objective is to provide temporary storage, computation, and other services like communication, control, storage, configuration, measurement, and management. SG is moving from central to the decentralized type of infrastructure [15]. Services are very much advantageous in SG environment like real time processing and response and dynamically allocation of resources on requirement of SG devices, which is also called resource pooling. Fog computing has four main advantages which can be useful for the resolution of the certificate verification problem in IoT networks [16]. (1) Cognition: It means Fog architecture is aware of the edge user requirement. Fog decides about computing, storage, and control functions placement. (2) Efficiency: The best utilization of available resources by pooling resources. (3) Agility: Fog is much more scalable in the deployment and operation of new services; this supports rapid innovation. (4) Latency: Latency issues are resolved for real-time applications.

In addition to the above-mentioned advantages, fog computing has security issues as well. Similarly, fog computing can still play a vital role in the improvement of the digital certificate verification process [17]. In addition, fog nodes capacity may vary from limited resources to high power computational device(s). The revolutionary changing and implementation requirements at the edge layer have overridden the concept of cloud computing with fog computing. The SG devices or edge devices have mostly limited resources like processing power, storage, bandwidth, battery, and require to give real-time response [5] for real-time transactions. The time duration is less than milliseconds for information to be useful. For example, health or temperature information about the electric component. Therefore, fog computing is the most suitable solution, where processing is performed close to edge devices and this architecture fulfills the requirements of Certificate Revocation Information among SG Devices.

Short-Lived Certificate (SLC) is another way of certificate verification. SLC are issued for short time, i.e., 1–3 Days [18] and due to the short lifetime there is no need for certificate revocation list (CRL) or online certificate status protocol (OCSP) because compromised certificates are set to expire before browsers would check for CRL or OCSP status. This creates difficulty for the attacker because browsers do not have to check for certificate status, SLC enables faster web load times as well as enables reliability on OCSP response is excluded and this provides prevention against a man-in-the-middle attack. SG infrastructure is being increasingly used for providing reliable services to consumers in an efficient and secure way [19]. SG is one of the most significant application of IoT [20]. SG installations and implementations are always an attractive choice for attackers [21]. With the rapid growth in IoT and SG devices, there are many security issues highlighted from time to time [22,23]. Security requirements are also increased with time. There are many security issues highlighted specifically for SG in [20,24,25]. In the past security services were Confidentiality, Integrity, and Availability (CIA)-triad, which referred as confidentiality, Integrity and availability or authentication. These are no more sufficient to address the latest requirements and proposed IAS-octave [26]. Table 2 shows IAS-OCTAVE Service Achieved Using Digital Certificates.

Table 2. IAS-OCTAVE services achieved using digital certificates.

Ser	Service Name	Digital Certaddress?	How Digital Cert Achieve Service
1	Confidentiality	Yes	Secure exchange of Symmetric Key and Asymmetric Encryption
2	Integrity	Yes	Cryptographic hashes encrypt with private key
3	Availability	Yes	Protection against DoS Attack
4	Accountability	Yes	Usage of Private Keys
5	Auditability	Yes	Partial
6	Trustworthiness	Yes	Root CA and intermediate CA
7	Non-repudiation	Yes	Usage of Private Keys
8	Privacy	Yes	Secure exchange of Symmetric Key and Asymmetric Encryption

Various key management systems are discussed in [27], which tells importance of key management system in achieving security services. PKI is one of the comprehensive solutions to provide security services to various types of ICT (Information and Communication Technologies) devices including edge devices at a different cost in terms of processing and communication overhead. The secure use of PKI is dependent on the correct use of Digital Certificates. Digital Certificates can be used to resolve most of the security issues and are useful in achieving security services. The most important and vital component in SG infrastructure is the edge device, which is required to be secured. When any single device is compromised, then the whole grid can be exploited by attacker [3]. Edge devices are vulnerable to hardware Trojans, Side-channel attacks, Denial of Services (DoS), Physical attacks, Node replication attacks, Camouflage, and Corrupted node [26]. Digital certificates are suggested as a countermeasure to application-level attacks [21,28,29]. Most of these services can be achieved effectively only if edge devices are updated about the certificates which are revoked. One important issue is the distribution of certificate revocation information among SG devices or edge devices.

The rest of the paper is organized as follows. Section 2 is about the review of existing certificate revocation schemes (i.e., CRL and OCSP) and critical analysis of existing schemes in the context of the SG environment and requirement of an efficient certificate revocation scheme. In Section 3, we propose a scheme, Fog Node as an Intermediate Certification Authority (FONICA), suitable for an SG environment based on established performance parameters (storage and communication overhead). Further, in Section 3, the overview, workflow, messaging, and numerical analysis of the purposed scheme are described in detail. In Section 4 results are calculated for Performance parameters and compared with other benchmark schemes. Section 5 describes the critical analysis of the proposed scheme. Finally, Section 6 concludes on the overall efficiency and benefits of the proposed scheme.

2. Literature Review

Two main certificate verification schemes are currently being used in the internet are Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP). These schemes follow mostly X.509 certificate format and different fields of X.509 Certificate, CRL fields, OCSP request, and OCSP response fields are described in [30].

CRL mechanism works as follows: CA issues periodically a CRL list signed by CA, which contains a list of all the revoked certificates. These certificates may be revoked by CA due to any reason. For example, the information of the certificate owner is changed, and thus the respective private key is compromised or any other reason by which the owner of the certificate is no more trusted. This mechanism is not suitable for edge devices because over time CRL grows, the size of CRL may vary from 793 bytes to 5 MB [5]. This requires huge processing and consumes the storage and power of edge devices. OCSP is an online certificate verification scheme in which clients request verification against the certificate's serial number. OCSP server responds after checking the status of the certificate. Although OCSP has resolved the issues of storage and power consumption. However, this scheme is also not good for the distribution of certificate revocation information due to the latency issue. Edge device must request for each new certificate and OCSP server takes time in responding. It is stated that the median time taken by the OCSP server is 291 ms [31], while delay time is tens of milliseconds for edge devices involved in online transactions [16]. Specifically, in a SG environment where transaction leads to financial impact. Therefore, some efficient schemes must be required for the distribution of certificate revocation information.

Various Digital Certificate Revocation schemes are recently proposed and improved certificate revocation mechanism [4,32–36]. However, keeping in view the SG environment and energy efficient devices, these schemes still can be improved. Here are a few most recently proposed certificate revocation schemes and their limitations in a energy efficient environment. The first scheme uses "Bloom filter", the scheme has four components, i.e., cloud, CA, fog node, and edge node. The fog node is responsible for the distribution of certificate revocation information of CA (s). "Bloom filter" [5] is used to reduce the size of CRL. The received CRL from multiple CA is forwarded to the intended fog node, then the fog node formulates bloom filter and forwards it to edge devices. Each node verifies the certificate using bloom filter and in case of probabilistic decisions edge node approaches fog node for certificate status. This technique has improved in the context of storage, which is one main issue of SG devices. However, these SG devices are still required processing for the calculation to get information from the bloom filter. The fog node will send only the bloom filter and the edge node must calculate itself. This processing cost in terms of power consumption on edge devices and battery life of such devices is still an issue. Another issue with this recently proposed scheme is that, it requires implementation changes for the inclusion of the bloom filter.

Another scheme is the certificate less scheme introduced as "Twin-Peaks" in [32]. In this scheme, public keys rely on the public information of the owner, for example domain name and IP address. A hierarchical structure of key server parallel to DNS hierarchy is suggested. This approach seems to be very suitable for SG environment, but this requires again a complete infrastructural change and huge overhead of complete hierarchy. Another recently published Scheme is "Secure Guard" [4]. This scheme verifies during Transport Layer Security (TLS) handshake. ISP is also involved in this scheme. Whenever the end-user establishes a connection with ISP a cache server at ISP will validate the certificate during TLS handshake. This scheme also requires the additional overhead of cache servers at the ISP level. A scheme recently proposed for Advanced Metering Infrastructure (AMI) in [34]. In this scheme distributed CRL management scheme utilizes distributed hash trees (DHTs). The scheme inherits built-in drawbacks of CRL and most specific for the environment like peer-to-peer infrastructure, SG environment may vary and much diverse.

Short-Lived Certificate (SLC) scheme is one of the suitable solutions for SG environment. In this scheme, digital certificates of X.509 are issued for a specific period and CA issues a new certificate at the end of the validity period. This period is defined as average caching time, which is reported as four days in [35]. SLC has nine fields and uses Elliptic-curve cryptography (ECC). This scheme has reduced the overhead of the certificates verification process during the establishment of the connection. This scheme has two main issues reported, first is heavy resource utilization at the server end and the second issue is linked with the increase in the number of certificates because the number of devices is continuously increasing. Ad-hoc Distributed OCSP for Trust (ADOPT) is an advanced version of SLC proposed by Masdari, in which the validity period of SLC is changed on basis of the behavior of the certificate owner [37]. However, this scheme has also an issue because OCSP responses are refreshed again and again, this will increase processing and messaging overhead [37]. Publish/subscriber-based version of the ADOPT (PS-ADOPT) certificate validation scheme has improved inconsistency about revoked certificates but two cache servers are introduced and require frequent communication between the edge node and OCSP responder [36]. Recently Masdari proposed the Markov-chain model, again this model has issue for using with energy efficient devices because of mathematical processing required for the probabilistic approach. Rev Cast is one of the best techniques for the distribution of certificate revocation information among SG devices over wireless radio signals proposed in [38]. This technique is useful for devices that contains embedded FM antenna. Implementation of this scheme must also work for distributed nature of SG devices.

Lightweight X.509 Digital Certificates compresses the certificate fields and removes of duplications also. This scheme is proposed in [39]. There are many alterations proposed in the scheme but one of the modifications is the merging of signature and signature Algorithm. The signature field that a CA uses to sign its own certificate or generated own signature while on the other hand signature algorithm uses for client's certificate and both fields are mostly same. Merging these fields CA must use the same algorithm for both purposes. The proposed scheme has omitted both the signature and the signature algorithm fields and fixed them to ecdsa with SHA256. Datagram Transport Layer Security (DTLS) also uses the same algorithm. Following Table 3 shows a comparison of already proposed schemes in terms of efficiency parameters.

Table 3. Comparison of Issues in existing Schemes.

Ser	Scheme	Storage Issue	Processing Issue	Latency Issue	Communication Overhead	Remarks
1	CRL	✓	✓	×	✓	CRL Size is issue
2	OCSP	×	✓	✓	✓	Latency is issue
3	Bloom filter	×	✓	✓	✓	Processing at edge node is issue
4	Twin-Peaks	×	✓	×	✓	Require infrastructure change
5	Secure Guard	×	✓	×	✓	Require infrastructure change
6	Distributed hash trees	×	✓	×	✓	Specific for Peer to Peer infrastructure
7	Short Lived Certificate	×	✓	×	✓	Huge Processing at Server
8	Lightweight X.509 Cert	×	✓	×	✓	Signature and the signature Algorithm fields are fixed to ECDSA with SHA256

Keeping in view IAS-octave's security requirement, i.e., Confidentiality, Integrity, Availability, accountability, Auditability, trustworthiness, Non- repudiation and Privacy, and summary of above-described schemes. Similarly, the SG environment requires a more efficient scheme in which energy efficient devices may verify certificate status with an efficient storage, processing, and minimum communication over the network.

3. Problem Statement and Contribution

3.1. Problem Statement

Security services are essential to be achieved for SG infrastructure with resource efficient techniques. Existing techniques for distribution of information about revoked certificates are CRL, OCSP, and "Bloom Filter". These schemes are also called digital certificate verification schemes. CRL and OCSP are currently being used widely over the internet. First is CRL technique, which consumes storage on edge device as well as require processing for certificate verification on edge device. Second is OCSP technique, which requires time to request and response for verification of each certificate. This technique is not suitable for real-time environment such as SG. Third one is a recently proposed technique, i.e., "Bloom Filter". This technique has resolved issues of both previous techniques but require protocol changes at edge device and CA side for implementation. So, this technique can also be improved. Therefore, a better scheme is essentially required to be proposed to meet latest security challenges in resource efficient way. This phenomenon can be improved in term of storage and processing. Efficient distribution of information about revoked certificates among edge devices in a SG environment in a resource efficient way is a challenging job.

3.2. Contribution

A novel scheme has been proposed after a thorough literature review and critically analyzing security requirements of SG infrastructure. It was seemed appropriate that fog computing along with SLC can be used to meet security requirements in a resource-efficient way. In the proposed scheme, existing techniques are integrated with the concept of SLC using fog computing. Complete architecture, flow chart, and messaging mechanism of the scheme are described. The proposed scheme is compatible with existing techniques. Mathematical Equations (1)– (3) and (6) are taken from recently proposed literature while (4), (5) and (7) are formulated to compute storage overhead. CRL and "Bloom filter" techniques are compared with the proposed scheme in terms of storage overhead. OCSP and "Bloom filter" techniques are compared with a proposed scheme in terms of communication overhead. The proposed scheme has shown better results with much security strength. The scheme has resolved many security issues in a resource efficient way.

4. Materials and Methods

4.1. Background

First, the core objective of the proposed scheme is to provide a foolproof security to achieve all security services efficiently using transport layer security protocol DTLS or SSL. In DTLS or SSL protocol during handshake phase server shares its certificate for own authenticity and client verify its certificate through respective CA using CRL or OCSP. In this way after successful verification of server's certificate connection establishes. Another important aspect during handshake process is authenticity of client side using client's certificate, which remains generally an optional component. In SG and IoT infrastructure client side certificate is very important because of machine to machine communication. The proposed scheme is specifically designed to address requirements of IAS octave for each side of M2M communication, which is not being achieved using any implementation of certificates. SG infrastructure must be real-time and two-way communication [40]. This security strength achieved using proposed scheme. Because issuing of certificate for each edge device is a huge overhead and there will be 28.5 billion networked devices by 2022 [41].

Secondly, edge devices of SG infrastructure mostly require communication among each other instead of cloud. Four phases SG infrastructure are generation, transmission, distribution, and consumption [20], which covers complete cycle from energy generation SG to consumption at consumer end for a specific area. In these phases each component is required to communicate with each other most of the time. For example, dynamic pricing during the peak hours should be automatically updated at grid level as well as Advance metering infrastructure (AMI) should also be integrated. Smart meters should intimate about consumption of energy. Distributed generation of energy resources from customer's end also requires to integrate with SG. The most important homes connected with SG to intimate consumption detail and demand management [41]. Similarly, for conceptual understanding edge devices at home, for example, remote control, refrigerator television, microwave oven, heater, air conditioner, and fan are required to communicate locally and they have nothing to do with cloud unless specifically required to access by owner when out of the home or any other specific task. In Figure 1, depicted that most of edge devices are required to communicate locally with each other.

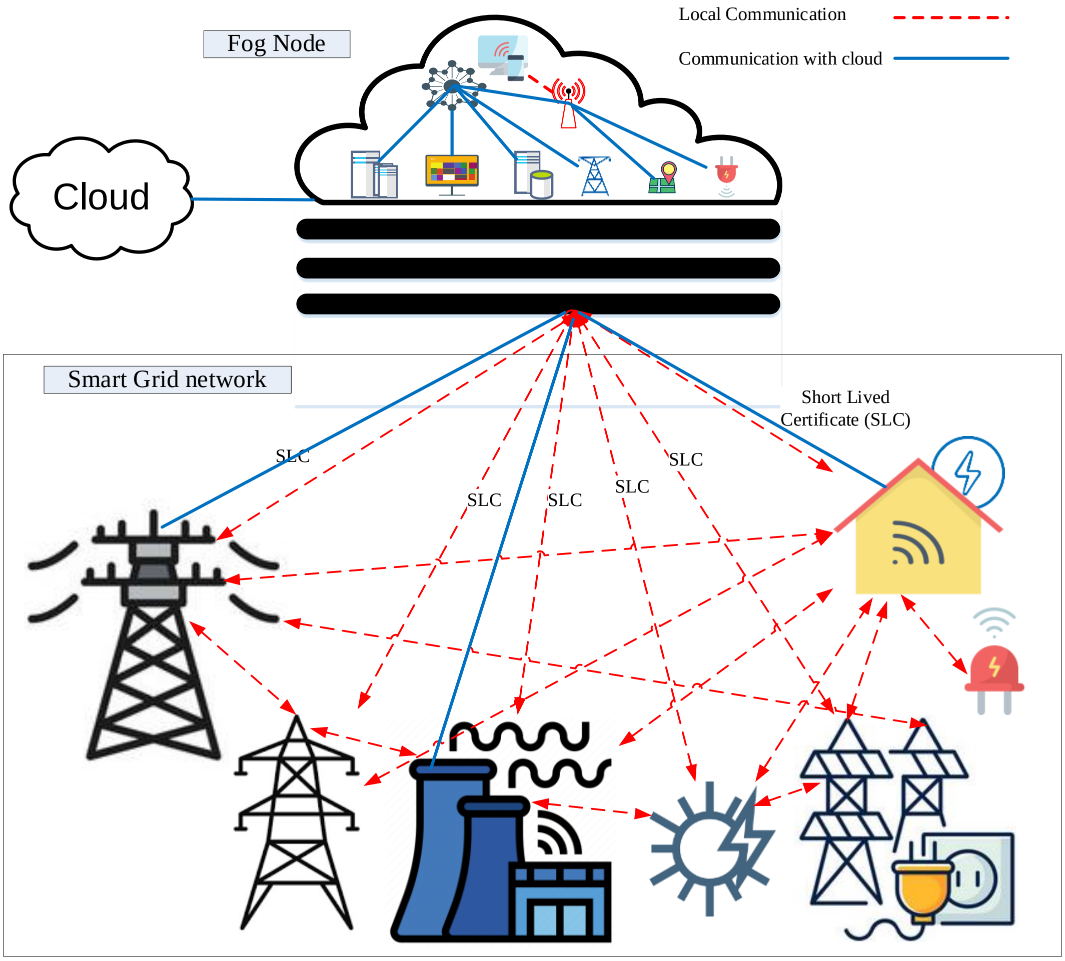

Figure 1. FONICA Communication.

4.2. *Overview of the Proposed Methodology*

The proposed scheme will reduce storage consumption on edge devices, communication overhead, latency time, and processing requirements for certificate verification in the SG environment. The scheme is based on fog computing architecture. This scheme requires no major modification to existing infrastructure. The fog node will be acting as an Intermediate Certification Authority (FONICA). Further, the FONICA is trusted by all edge devices under the area of this Fog node. Area of fog node may be defined based on geographical location or administrative control. Fog area can be a university campus, airport, hospital, or corporate office. When a new edge device enters in an area of FONICA's trusted domain and tries to connect Fog node. Immediately Certificate of FONICA (CERT-FONICA) will be verified using a conventional process. Figure 2 shows an abstract level view of the proposed scheme within fog computing architecture. The fog node which is called FONICA is issuing SLC to edge nodes.

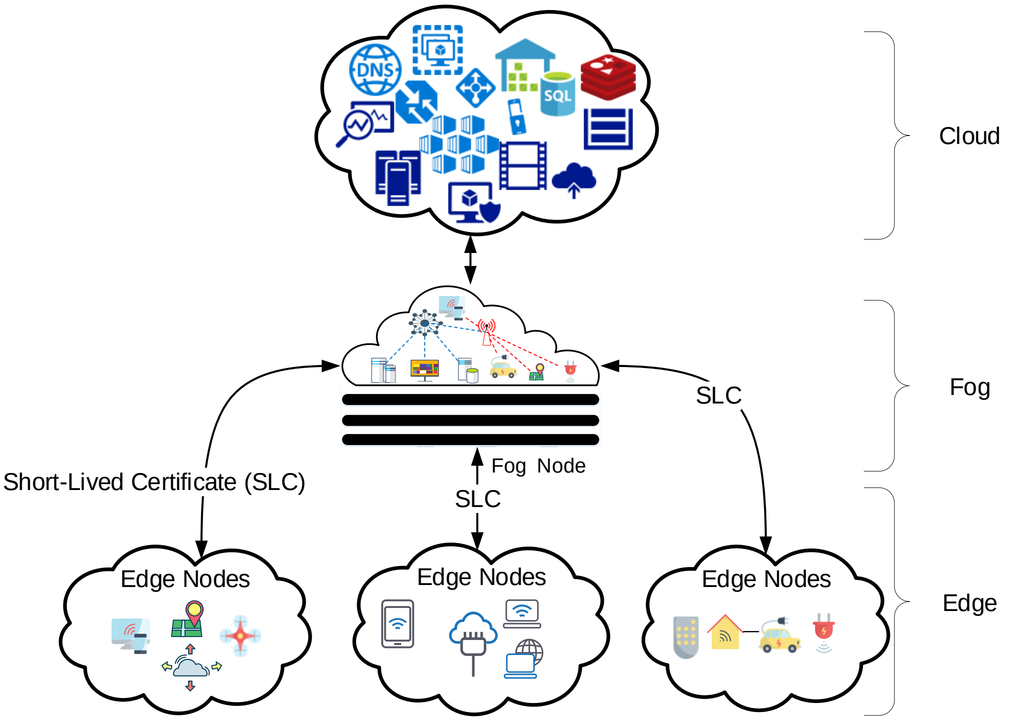

Figure 2. Proposed Architecture (FONICA).

FONICA will issue SLC to all edge devices for a lifetime of one day and whenever a certificate is revoked immediately a new certificate will be issued. It is highlighted by ABI Research that 90% of data is stored and processed locally instead of sending on the way to clouds [42]. This is a clue for the focus on the protection of 90% of communication among edge devices. This communication has nothing to do with the cloud.

This scheme will be effective for those edge devices, which requires frequently SSL, TLS, and DTLS handshake during connection establishment within a trusted area of FONICA. The edge devices within a trusted area of FONICA does not require any verification because SLC will be issued in case a certificate is revoked. Revocation information is maintained on FONICA but no need to transmit among edge devices. Whenever edge devices found FONICA as CA then immediately establish a connection and no need for a certificate verification process. This will minimize communication overhead on the network as well as eliminate storage overhead on edge devices. However, when a new edge device will join a trusted domain the certificate verification process for FONICA will be the same. This makes FONICA to be trusted. The scheme will be effective when an edge device requires more than one handshake within the trust domain. It can be easily deduced from Figures 1 and 2 that the distribution of SLC from FONICA will eliminate the communication overhead and latency at the time of connection establishment.

Specifically, Figure 1 has depicted that 90% of data generation and processing is done locally without the involvement of the cloud. Other 10% of communication requires to communicate outside the area of fog. Consequently, the verification process for 90% of communication is eliminated.

However, in case of communication required over internet delay will be same as routine communication required. Red dashed lines in Figure 1 are showing communication trusted by FONICA which is a local CA. Blue dashed lines in Figure 1 are showing communication trusted by a third party CA (IdenTrust, Comdo, DigiCert, etc). There are various edge devices that are not required to be connected other than pre-defined functioning requirements. For example, Remote control of Air condition and televisions, electric switches with the sensor, VANET (Vehicular ad hoc network) and sensor on refrigerator etc.

OCSP was facing issue of latency while the issue with CRL scheme was increased size of CRL and its storage on energy efficient devices. Both the issues are resolved in the way that latency is reduced by local CA and storage issue resolved by issuing SLC where no requirement of storing CRL on edge devices is there.

4.3. Work Flow of the Proposed Methodology

The scheme works in the way whenever an edge device starts establishing a connection with any other edge device or server. First, it verifies the certificate during handshake whether the certificate is issued by FONICA then it is assumed that the certificate is trusted because FONICA issues a new certificate on the revocation of any certificate. In other cases, when a certificate is not issued by FONICA, its verification process will follow the respective CA's implementation scheme. CA's scheme may be CRL based or OCSP based. The same process is depicted in the flow chart in Figure 3. This scheme ensures secure communication between edge devices within the domain of FONICA. The proposed scheme establishes a trusted domain for trusted edge devices. The scheme also addresses the case when an untrusted edge device becomes part of the trusted domain. In such a case edge device is required to present a valid certificate and verify the certificate of FONICA. Later, there is no certificate verification process for communication within a trusted domain. Devices within the trusted domain will be having SLC and not require a verifying certificate at the time of connection establishment

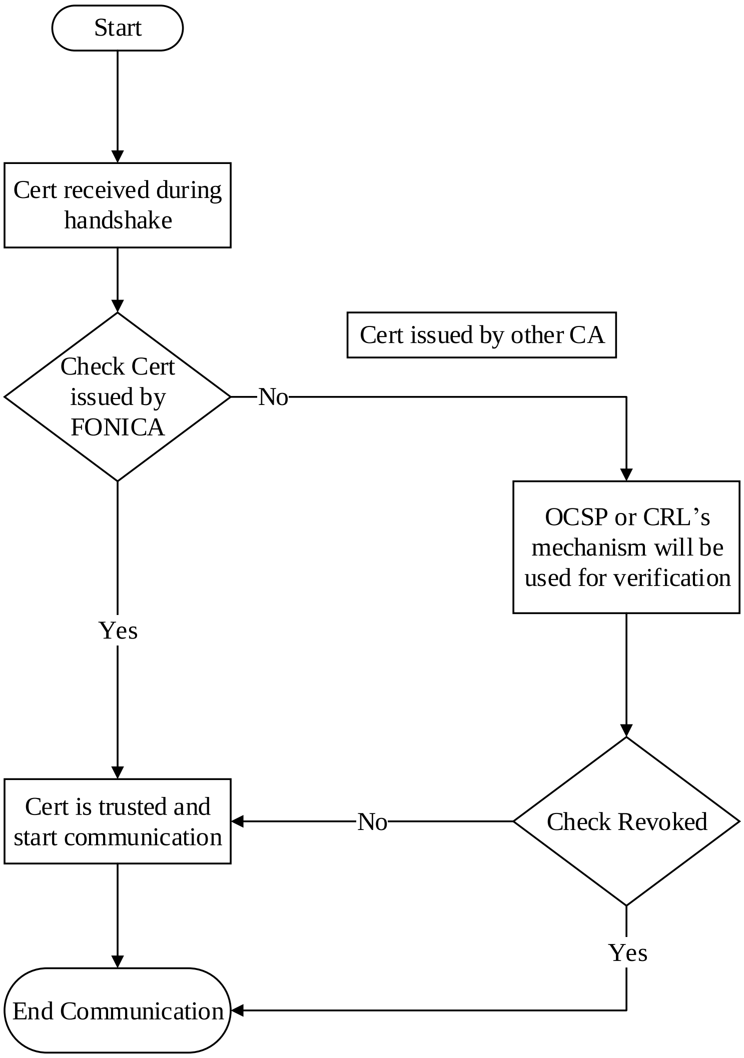
Start
Cert received during handshake
Check Cert issued by FONICA
Cert issued by other CA
No
OCSP or CRL's mechanism will be used for verification
Yes
Cert is trusted and start communication
No
Check Revoked
Yes
End Communication

Figure 3. Workflow of FONICA.

4.4. Messaging System in the Proposed Methodolgy

Figure 4 illustrates the messaging between edge nodes, fog nodes, and CA. Initially, it is assumed that the Fog Node contains information about the CRL of all relevant CAs. Node-1 establishes a connection with the Fog Node and verifies its certificate using a traditional certificate verification scheme. Node-1 verifies the certificate of Fog Node using a public key of CA. Once Fog Node becomes trusted and its chain of trust is verified then it may work as an intermediate CA. Now, the fog node is capable of issuing SLC to edge devices. SLC is duly signed by a private key of Fog Node and Node-1 will verify using a public key of Fog Node. Similarly, Node-2 verifies the certificate of Fog Node using a public key of CA. Once Fog Node becomes trusted then it may work as an intermediate CA and capable of issuing SLC to Node-2. SLC is duly signed by a private key of Fog Node and Node-2 will verify using a public key of Fog Node. Now, Node-1 and Node-2 are in the same trusted domain, and the certificate of Fog Node is placed at edge device like other CA's certificates.

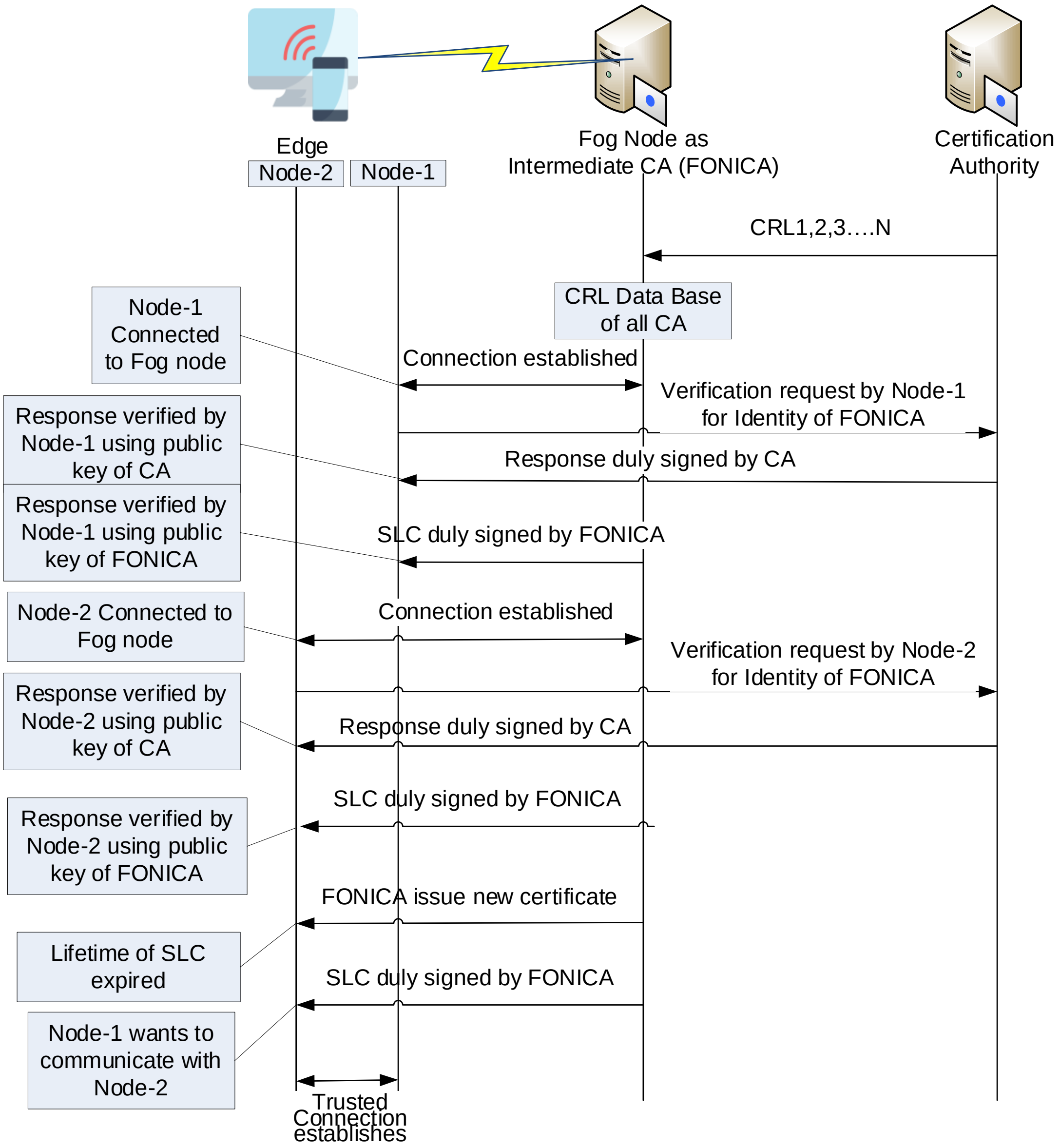
Edge
Node-2
Node-1
Fog Node as Intermediate CA (FONICA)
Certification Authority
CRL1,2,3….N
CRL Data Base of all CA
Node-1 Connected to Fog node
Connection established
Verification request by Node-1 for Identity of FONICA
Response verified by Node-1 using public key of CA
Response duly signed by CA
Response verified by Node-1 using public key of FONICA
SLC duly signed by FONICA
Node-2 Connected to Fog node
Connection established
Verification request by Node-2 for Identity of FONICA
Response verified by Node-2 using public key of CA
Response duly signed by CA
Response verified by Node-2 using public key of FONICA
SLC duly signed by FONICA
FONICA issue new certificate
Lifetime of SLC expired
SLC duly signed by FONICA
Node-1 wants to communicate with Node-2
Trusted Connection establishes

Figure 4. Messaging of FONICA.

4.5. Numerical Analysis

Numerical analysis is focused on storage issue with CRL and latency issue with OCSP. Latency will be having a huge impact because in fog architecture edge devices are mostly connected directly with FONICA. In the case of the cloud, OCSP request is served after 14xhops in our lab experiments. Therefore, real-time applications will be facing no delay during connection establishment. One study has shown that the median OCSP responder time is about 291 ms [5]. In the case of FONICA, it is 0 ms because SLC does not require any verification time.

The variables in following Table 4 are used in mathematical work are as follows: T_{CRL}, T_{BF} and $T_{FONICA.CRL}$. These variable shows a total number of bytes used by CRL, Bloom filter, and FONICA scheme, respectively, for "N" number of edge devices. The equations mentioned below are for computation of storage overhead of CRL, Bloom filter, and FONICA. The results are calculated by considering (N = 1000), i.e., 1000× edge devices are connected within the domain of FONICA. The no of revoked certificates is 1–50.

Table 4. Variables description for numerical analysis.

Variable/Symbol	**Description**	**Values of Variables**
B	No of revoked Cert	b = 10, 30 and 50
N	Total no of nodes under Area of FONICA	N = 1000
S	Serial No. Certificate	S = 20 bytes
T_{CRL}	Total storage will be consumed by edge devices for CRL Scheme	$N \times ((b \times 20 + 700))$ bytes
T_{BF}	Total storage will be consumed by edge devices for Bloom Filter Scheme	$T_{BF} = N \times \frac{-b\ .\ ln\ (p)}{\left(\ln(2)^2\right)}$
T_{OCSP}	Total communication overhead for edge devices for OCSP Scheme	$N \times (292)$ bytes
$T_{FONICA.CRL}$	Total storage will be consumed by edge devices for FONICA Scheme with CRL implementation.	$T_{FONICA.CRL} = (b - (b \times 0.1)) \times Cert\_Size + (b \times 0.1 \times T_{CRL}))$
$T_{FONICA.OCSP}$	Total communication overhead for edge devices for FONICA Scheme with OCSP implementation.	$T_{FONICA.OCSP} = (b - (b \times 0.1)) \times Cert\_Size + (b \times 0.1 \times T_{OCSP}))$
P	p is the chosen probability of a false positive, which is 0.01 in Bloom Filter experiment	P = 0.01
Cert_Size	54 x Certificates collected and average certificate size is considered for computations.	Cert_Size = 1054 Bytes

The following equations are derived for computation of storage and communication overhead. Equation (1) shows the size of CRL that will be distributed among N× edge devices. The CRL file size is based on certificate's serial number size (15 to 20 bytes), and the CA's signature size (700 bytes). Therefore, total CRL file size is b × 20 + 700 bytes. Then Equation (2) shows the overall storage overhead for N x devices. Equation (3) shows the overall storage overhead of the Bloom filter scheme. Likewise, Equations (4) and (5) are showing storage overhead. The left portion of the equation is showing 90% communication when CA is FONICA and the right portion of the equation is showing when CA is other than FONICA. In case when CA is other than FONICA then CRL of respective CA (Equation (4)) will be shared with specific edge devices or edge device may verify certificate using OCSP (Equation (5)). In Equations (2) and (3) storage overhead is computed by just multiplying already proposed equations in bloom filter with a total number of edge devices under the area of the fog node. In Equations (4) and (5) first part is showing that only one certificate is required for each edge device on revocation instead of communicating CRL to each device, i.e., $(b - (b \times 0.1)) \times Cert\_Size$. The second part is showing that only 10% of edge devices are required communication outside the area of the fog node using CRL or OCSP, i.e., (b×0.1× TCRL) or (b×0.1× TOCSP). In Equation (6) TOCSP is formulated by just multiplying request and response size (292 bytes) with a total number of edge devices to compute total communication overhead for certificate verification in the OCSP Scheme.

$$\text{Size of CRL} = (\text{b} \times 20 + 700)\ \text{bytes} \tag{1}$$

$$\text{T}_{\text{CRL}} = \text{N} \times ((\text{b} \times 20 + 700))\ \text{bytes} \tag{2}$$

$$\text{T}_{\text{BF}} = \text{N} \times \frac{-\text{b} \,.\, \ln(\text{p})}{(\ln(2)^2)} \tag{3}$$

$$\text{T}_{\text{FONICA.CRL}} = (\text{b} - (\text{b} \times 0.1)) \times \text{Cert\_Size} + (\text{b} \times 0.1 \times \text{T}_{\text{CRL}})) \tag{4}$$

$$\text{T}_{\text{FONICA.OCSP}} = (\text{b} - (\text{b} \times 0.1)) \times \text{Cert\_Size} + (\text{b} \times 0.1 \times \text{T}_{\text{OCSP}})) \tag{5}$$

Secondly, we formulate the following equations for the computation of communication overhead for OCSP, Bloom filter, and FONICA. OCSP, the protocol does not have any storage overhead, because it is an online approach. Packet size for an OCSP query is 292 bytes considering both the request and response packet sizes. Equation (6) is showing OCSP request and response size which is 292 bytes while Equation (7) is showing the total communication overhead of OCSP for N edge devices.

$$\text{Size of OCSP} = 292\ \text{bytes} \tag{6}$$

$$\text{T}_{\text{OCSP}} = \text{N} * (292)\ \text{bytes} \tag{7}$$

5. Results

The proposed scheme is simulated in Matlab and all results are generated from equations derived from the numerical analysis in the previous section. Equations (2)–(5) are showing the total storage requirement for N edge devices and on the assumption of "b" no of revoked certificates in one day. Equation (1) is the size of CRL for N edge devices. The CRL is required to be distributed among N edge devices and Equation (2) shows total storage consumption with respect to CRL for N edge devices. Equation (3) is the formula of Bloom Filter's storage calculation. The Equation (4) is a storage consumption with respect to FONICA for N edge devices. The equation is comprehensively covering both cases when 90% of communication is covered by short-lived certificates while 10% of the remaining communication is covered using the existing scheme. When the existing scheme is CRL-based then Equation (4) is covering otherwise for OCSP Equation (5) will be used to compute storage overhead. Figure 5 shows a comparison of storage consumption of three schemes (CRL, Bloom Filter and FONICA). The x-axis of Figure 5 shows a number of revoked certificates in a day and y-axis shows storage consumption in bytes.

The results from Figure 5 depicting that the bloom filter has improved storage consumption with respect to the CRL scheme. However, FONICA has reduced storage consumption on edge devices because there is no need to maintain a record at edge devices. The FONICA will keep track of revoked certificates and immediately issue new certificates whenever a certificated is reported revoke.

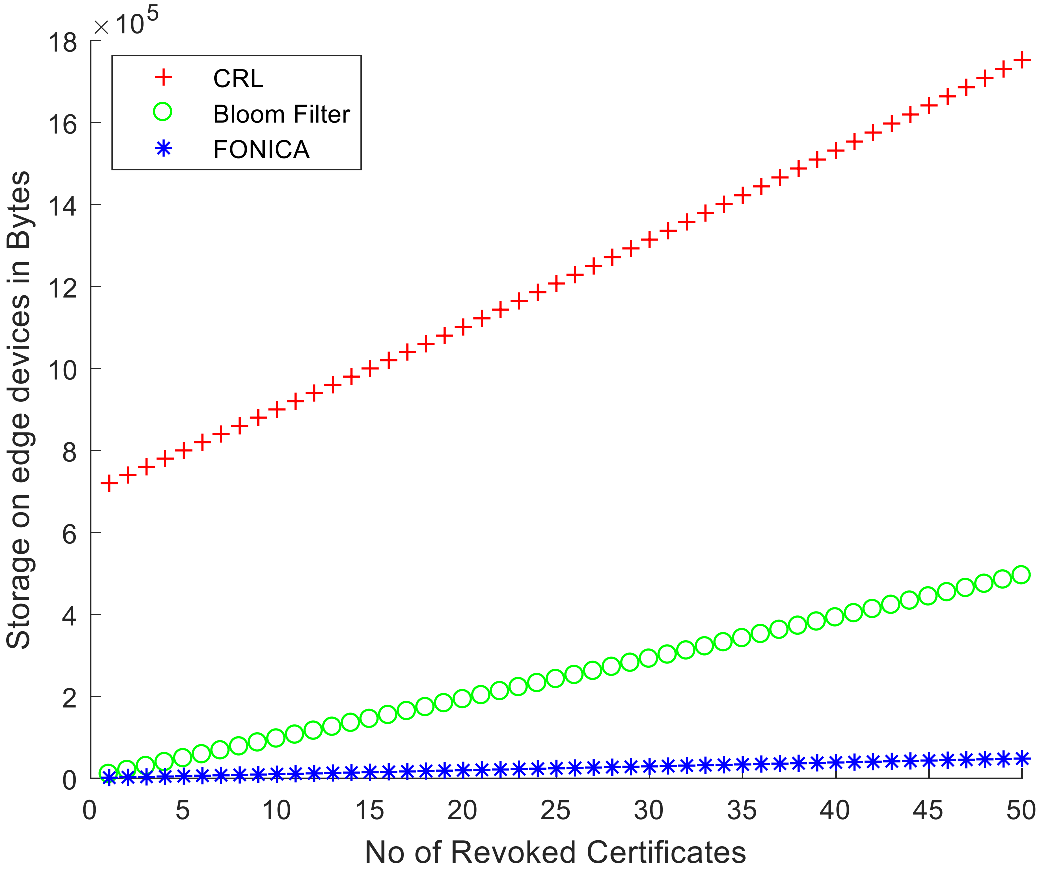

Figure 5. Storage overhead Comparison.

The Figure 6 is depicting communication overhead of 1000× edge devices. The CRL scheme is not compared because it does not incur overhead in communication at the time of connection establishment. The x-axis of Figure 6 shows a number of revoked certificates in a day and y-axis shows communication overhead in bytes. OCSP is not affected by a number of revoked certificates therefore Figure 6 shows the OCSP line straight. However, bloom filter size keeps on increasing as a number of revoked certificates increases. On the other hand, FONICA is not much affected by a number of revoked certificates because a new certificate will be issued whenever a certificate is reported to be revoked. Therefore, FONICA incurs the least communication overhead because the only size of the certificate is considered as communication overhead. Figure 6 shows that FONICA has the least communication overhead. In other words, it can be easily explained that whenever an edge device is required to verify a certificate it simply generates an OCSP request and get an OCSP response and it does not matter that how many certificates are revoked. Figure 6 is depicting the same with a straight line which is showing for 1000× edge devices and number of revoked certificates varies from 1 to 50. The Bloom filter size keeps on increasing as no of revoked certificates increases. FONICA is also affected by the increasing no of revoked certificates but that is a very minor communication overhead which is depicted in Figure 6.

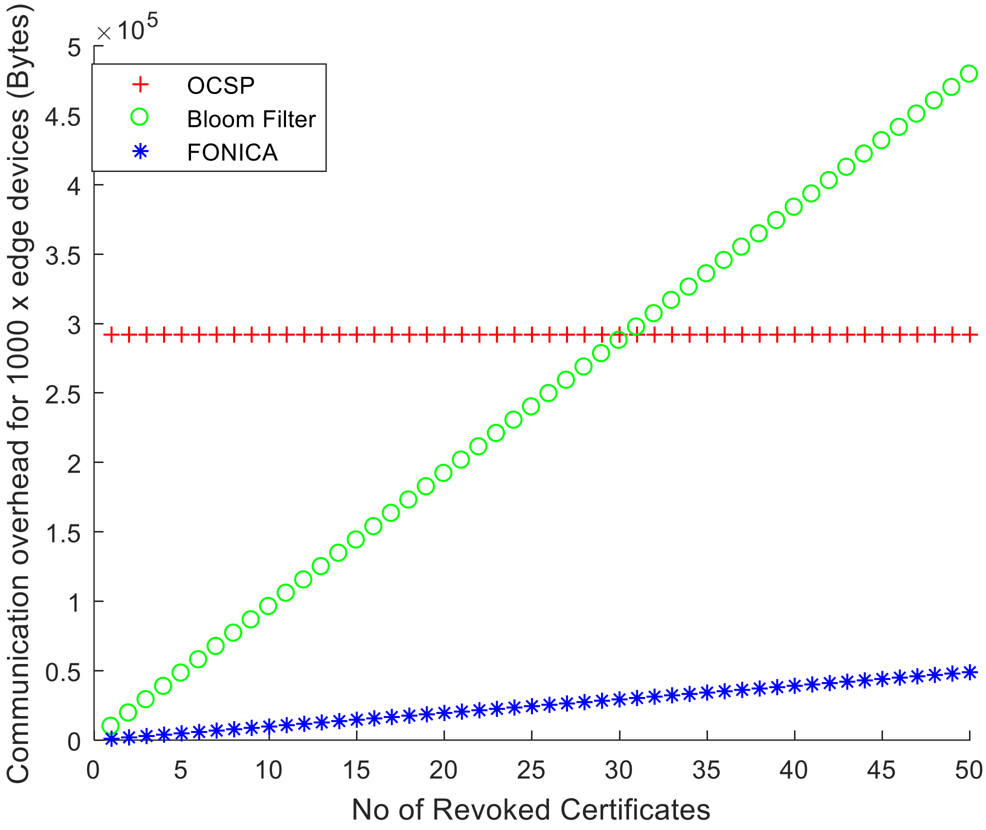

Figure 6. Communication overhead Comparison.

The calculations and results are shown in Figures 5 and 6 are based on the supposition for 1000× edge devices in terms of storage and communication overhead, respectively. While a number of edge devices may differ in realistic deployment of fog computing infrastructure. Keeping in view this variation, calculations are made for variation in a number of edge devices.

The Figure 7 given below shows results of calculation for edge devices ranging from 100 to 5000× edge devices. The x-axis of Figure 7 shows number of edge devices and y-axis shows storage and communication overhead in bytes. Figure 7 compares the overall efficiency of FONICA with CRL, OCSP, and Bloom Filter. CRL and Bloom filter scheme is compared in terms of overall storage consumption for a number of edge devices ranging from 100 to 5000. While the OCSP and Bloom filter scheme is compared in terms of overall communication overhead for number of edge devices ranging from 100 to 5000. It can be easily depicted from Figure 7 that FONICA is much efficient in terms of storage consumption and communication overhead for different number of edge devices. Figure 7 also depicts the efficiency of the scheme while an increasing number of edge devices. Performance of the other existing schemes decreases as the number of edge devices increases. Bloom filter and OCSP are initially close to FONICA but when number of edge devices increased their storage consumption and communication overhead keep on increasing. This behavior is not much suitable for an energy efficient environment. Therefore, keeping in view above mentioned discussion FONICA is the most suitable scheme for energy-efficient environment.

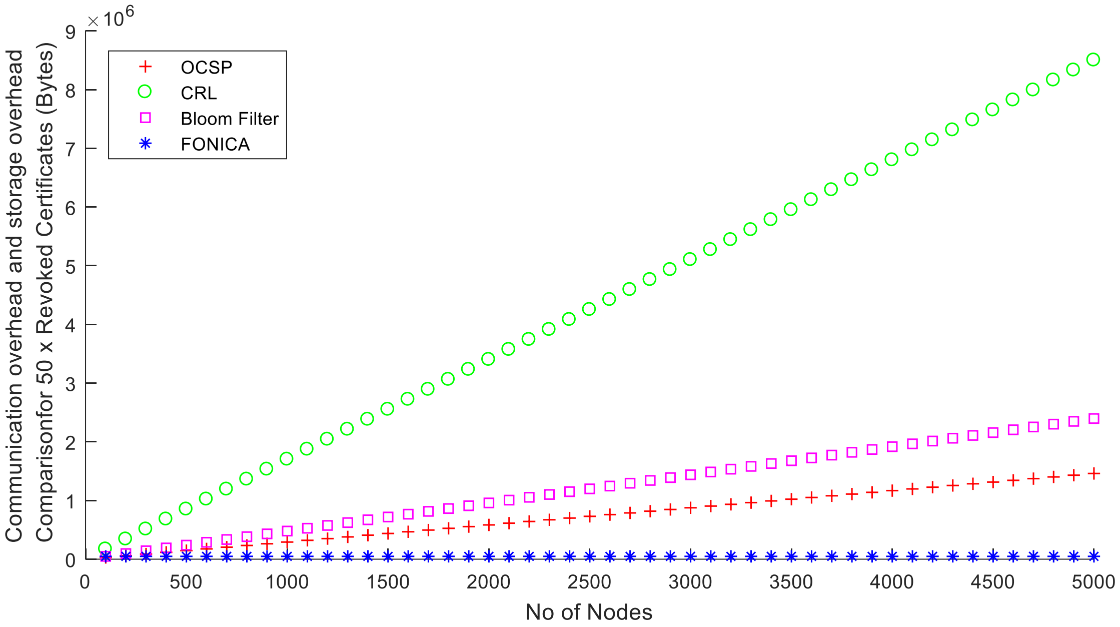

Figure 7. Storage and communication overhead for various edge devices.

The proposed scheme has also addressed the issue of latency because FONICA issues a new certificate when it is reported that the certificate is revoked within an area of fog node. As edge device must request for each new certificate and OCSP server takes time in responding. It is stated that the median time taken by the OCSP server is 291 ms [31]. In contrast, FONICA does not incur any latency issues. Ninety percent of verification requires 0 ms, which means no latency, and the remaining 10% of verification will incur the same 291ms. Therefore, the median time taken by FONICA's edge devices is 0 ms because most of the communication remains within the area of the fog node.

6. Critical Analysis of the Proposed Scheme

In the proposed scheme storage overhead is eliminated only for edge devices which remains under the area of a specific fog node for a long time, which is valid for SG infrastructure. The proposed scheme can be used to address security issues in the diverse nature of environments where IoT applications exist. This scheme is not much effective for VANET which moves frequently from the area of one fog node to another. In the case of VANET efficiency of this scheme will become equivalent to traditional CRL or OCSP, whichever is implemented. When SLC is issued by Fog node-1 and the vehicle moves to the area of fog node-2 then new SLC will be issued by fog node-2 after the edge device has verified the trust of fog node-2. This scheme has also a positive aspect for VANET when a vehicle moves into an area of fog node its one aspect is its global communication, i.e., GPS location, etc. There are so many other aspects required to be addressed locally. For example, in the case of congested traffic, vehicles are required to communicate frequently with geographically nearby vehicles to avoid accidents. This situation is easily elaborating that in the case of VANET vehicles not only requires communication globally but requires important communication locally within the area of fog.

Another critical aspect of this scheme is how PKI could be implemented in energy-efficient devices. PKI could be used effectively in energy-efficient environment in the way it is implemented on a requirement basis. For example, PKI can only be used for secure key exchange for symmetric communication. After secure key exchange, the session key can be used for bulk communication. Similarly, other security services such as authentication, Confidentiality, Integrity, Availability, Accountability, Auditability, Trustworthiness, and Non-repudiation can be achieved on a requirement basis.

The proposed scheme contributes to establishing secure and sustainable communication among trusted and un-trusted edge devices. One use case of a proposed scheme is after issuance of SLC to any edge device for further communication with other edge devices will make it sustainable against cyber-attacks. Any attacker wants to communicate need a valid certificate. Based on this scheme, implementation of TLS or DTLS is suggested in such a way that any edge device part of SG want to communicate with other device requires a valid certificate. This will ensure secure and sustainable communication using FONICA.

7. Conclusions

The FONICA is an efficient certificate verification scheme that has contributed to reducing storage and communication overhead. The two main contributions can be concluded in the way that; first, it solves the issue of immediate distribution of certificate revocation information among energy-efficient devices. This has eliminated 90% of communication overhead. However, in the case of 10% of remaining communication incur very ignorable overhead for both CRL and OCSP (whichever is being used). The results show that the proposed scheme is efficient with respect to the CRL and Bloom filter scheme in terms of storage overhead on edge devices. Secondly, OCSP was facing latency issue which is also improved as edge devices in the SG network are not required verification at the time of connection establishment. FONICA scheme provides efficient secure communication among edge devices within the trusted domain as well as for public untrusted devices by verifying chain of trust. This will counter most of the cyber-attacks, which could be launched on edge devices and attacker cannot establish connection even if managed to get connected with network by any mean.

Author Contributions: Conceptualization, S.M. and M.G.; methodology, S.M.; software, M.G. and J.-G.C.; validation, S.-J.K., M.K. and M.G.; formal analysis, J.-G.C., M.K. and S.M.; investigation, M.G., J.-G.C. and S.-J.K.; resources, S.-J.K.; data curation, S.M., M.G. and M.K.; writing—original draft preparation, S.M., M.G. and M.K.; writing—review and editing, M.G., S.-J.K., H.A. and J.-G.C.; visualization, S.M., M.G. and M.K.; supervision, J.-G.C. and S.-J.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the BK21 FOUR project (AI-driven Convergence Software Education Research Program) funded by the Ministry of Education, School of Computer Science and Engineering, Kyungpook National University, Korea (4199990214394), and this study was supported by the Brain Pool Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science and ICT (2019H1D3A1A01102987).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The study did not report any data.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Kitajima, S.; Mambo, M. Verifying the Validity of Public Key Certificates Using Edge Computing. In *International Conference on Security with Intelligent Computing and Big-data Services*; Springer: Cham, Switzerland, 2017; pp. 330–336.
2. Kim, S.M.; Lee, T.; Kim, S.; Park, L.W.; Park, S. *Book Security Issues on Smart Grid and Blockchain-Based Secure Smart Energy Management System*; EDP Sciences: Les Ulis, France, 2019; p. 01001.
3. Kimani, K.; Oduol, V.; Langat, K. Cyber security challenges for IoT-based smart grid networks. *Int. J. Crit. Infrastruct. Prot.* **2019**, *25*, 36–49. [CrossRef]
4. Alrawais, A.; Alhothaily, A.; Cheng, X.; Hu, C.; Yu, J. Secureguard: A certificate validation system in public key infrastructure. *IEEE Trans. Veh. Technol.* **2018**, *67*, 5399–5408. [CrossRef]
5. Alrawais, A.; Alhothaily, A.; Hu, C.; Cheng, X. Fog computing for the internet of things: Security and privacy issues. *IEEE Internet Comput.* **2017**, *21*, 34–42. [CrossRef]
6. Kakakhel, S.R.U.; Kondoro, A.; Westerlund, T.; Dhaou, I.B.; Plosila, J. Enhancing Smart Grids via Advanced Metering Infrastructure and Fog Computing Fusion. In Proceedings of the 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, 2–16 June 2020; pp. 1–6.

7. Pooja, M.; Yadav, M. Digital Signature. *Int. J. Sci.* **2018**, *3*, 71–75.
8. Forcan, M.; Maksimović, M. Cloud-fog-based approach for smart grid monitoring. *Simul. Model. Pract. Theory* **2020**, *101*, 101988. [CrossRef]
9. Mahmood, S.; Ullah, A.; Kayani, A.K. Fog Computing Trust based Architecture for Internet of Things Devices. *Int. J. Comput. Commun. Netw.* **2019**, *1*, 18–25.
10. Sarkar, S.; Chatterjee, S.; Misra, S. Assessment of the Suitability of Fog Computing in the Context of Internet of Things. *IEEE Trans. Cloud Comput.* **2018**, *6*, 46–59. [CrossRef]
11. Mukherjee, M.; Matam, R.; Shu, L.; Maglaras, L.; Ferrag, M.A.; Choudhury, N.; Kumar, V. Security and privacy in fog computing: Challenges. *IEEE Access* **2017**, *5*, 19293–19304. [CrossRef]
12. Stojmenovic, I.; Wen, S. The fog computing paradigm: Scenarios and security issues. In Proceedings of the Federated Conference on Computer Science and Information Systems, Warsaw, Poland, 7–10 September 2014; pp. 1–8.
13. Stojmenovic, I.; Wen, S.; Huang, X.; Luan, H. An overview of fog computing and its security issues. *Concurr. Comput. Pract. Exp.* **2016**, *28*, 2991–3005. [CrossRef]
14. Ekanayake, B.N.; Halgamuge, M.N.; Syed, A. Security and Privacy Issues of Fog Computing for the Internet of Things (IoT). In *Cognitive Computing for Big Data Systems Over IoT*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 139–174.
15. Mollah, M.B.; Zhao, J.; Niyato, D.; Lam, K.-Y.; Zhang, X.; Ghias, A.M.; Koh, L.H.; Yang, L. Blockchain for future smart grid: A comprehensive survey. *IEEE Internet Things J.* **2020**, *8*, 18–43. [CrossRef]
16. Chiang, M.; Zhang, T. Fog and IoT: An overview of research opportunities. *IEEE Internet Things J.* **2016**, *3*, 854–864. [CrossRef]
17. Tariq, N.; Asim, M.; Al-Obeidat, F.; Zubair Farooqi, M.; Baker, T.; Hammoudeh, M.; Ghafir, I. The Security of Big Data in Fog-Enabled IoT Applications Including Blockchain: A Survey. *Sensors* **2019**, *19*, 1788. [CrossRef]
18. Rowley, J. How Short-Lived Certificates Improve Certificate Trust. Available online: https://www.digicert.com/blog/short-lived-certificates/ (accessed on 4 February 2016).
19. Khan, H. Cyber Security Challenges in Smart Grids. 2020. Available online: https://doi.org/10.31224/osf.io/ua3wp (accessed on 23 June 2020).
20. Gunduz, M.Z.; Das, R. Cyber-security on smart grid: Threats and potential solutions. *Comput. Netw.* **2020**, *169*, 107094. [CrossRef]
21. Fritz, J.J.; Sagisi, J.; James, J.; Leger, A.S.; King, K.; Duncan, K.J. Simulation of Man in the Middle Attack On Smart Grid Testbed. In Proceedings of the 2019 SoutheastCon, Huntsville, AL, USA, 11–14 April 2019; pp. 1–6.
22. Kumar, V.; Kumar, R.; Pandey, S. LKM-AMI: A Lightweight Key Management Scheme for Secure two Way Communications between Smart Meters and HAN Devices of AMI System in Smart Grid. *Peer–Peer Netw. Appl.* **2020**, *14*, 82–100. [CrossRef]
23. Ahmadiahangar, R.; Rosin, A.; Palu, I.; Azizi, A. Challenges of smart grids implementation. In *Demand-side Flexibility in Smart Grid*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 1–15.
24. Ali, S.S.; Choi, B.J. State-of-the-Art Artificial Intelligence Techniques for Distributed Smart Grids: A Review. *Electronics* **2020**, *9*, 1030. [CrossRef]
25. Nejabatkhah, F.; Li, Y.W.; Liang, H.; Ahrabi, R.R. Cyber-Security of Smart Microgrids: A Survey. *Energies* **2021**, *14*, 27. [CrossRef]
26. Mosenia, A.; Jha, N.K. A comprehensive study of security of internet-of-things. *IEEE Trans. Emerg. Top. Comput.* **2017**, *5*, 586–602. [CrossRef]
27. Ghosal, A.; Conti, M. Key management systems for smart grid advanced metering infrastructure: A survey. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2831–2848. [CrossRef]
28. Ahmad, M.; Younis, T.; Habib, M.A.; Ashraf, R.; Ahmed, S.H. A Review of Current Security Issues in Internet of Things. In *Recent Trends and Advances in Wireless and IoT-enabled Networks*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 11–23.
29. Qureshi, K.N.; Iftikhar, A. 6 Contemplating Security. In *Security and Organization within IoT and Smart Cities*; CRC Press: Boca Raton, FL, USA, 2020; p. 93.
30. Cooper, D.; Santesson, S.; Farrell, S.; Boeyen, S.; Housley, R.; Polk, W. Internet X. 509 public key infrastructure certificate and certificate revocation list (CRL) profile. *RFC* **2008**, *5280*, 1–151.
31. Stark, E.; Huang, L.-S.; Israni, D.; Jackson, C.; Boneh, D. The Case for Prefetching and Prevalidating TLS Server Certificates. In Proceedings of the 19th Annual Network & Distributed System Security Conference, San Diego, CA, USA, 5–8 February 2012.
32. Cho, E.; Park, M.; Kwon, T. TwinPeaks: A new approach for certificateless public key distribution. Conference on Communications and Network Security (CNS), Philadelphia, PA, USA, 17–19 October 2016; pp. 10–18.
33. Cebe, M.; Akkaya, K. Communication-efficient Certificate Revocation Management for Advanced Metering Infrastructure. *arXiv* **2019**, arXiv:1902.04255. [CrossRef]
34. Cebe, M.; Akkaya, K. Efficient Certificate Revocation Management Schemes for IoT-based Advanced Metering Infrastructures in Smart Cities. *Ad Hoc Netw.* **2019**, *92*, 101801. [CrossRef]
35. Topalovic, E.; Saeta, B.; Huang, L.-S.; Jackson, C.; Boneh, D. Towards short-lived certificates. *Web 2.0 Secur. Priv.* **2012**, *2012*, 1–9. Available online: https://cseweb.ucsd.edu/~{}dstefan/cse127-winter19/papers/topalovic:towards.pdf (accessed on 24 May 2012).
36. Masdari, M. Markov chain-based evaluation of the certificate status validations in hybrid MANETs. *J. Netw. Comput. Appl.* **2017**, *80*, 79–89. [CrossRef]
37. Masdari, M.; Jabbehdari, S.; Bagherzadeh, J. Improving OCSP-based certificate validations in wireless ad hoc networks. *Wirel. Pers. Commun.* **2015**, *82*, 377–400. [CrossRef]

38. Schulman, A.; Levin, D.; Spring, N. RevCast: Fast, private certificate revocation over FM radio. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, AZ, USA, 3–7 November 2014; pp. 799–810.
39. Tschofenig, H.; Fossati, T. *Transport Layer Security (TLS)/Datagram Transport Layer Security (DTLS) Profiles for the Internet of Things*; IETF: California, CA, USA, 2016.
40. Delgado-Gomes, V.; Martins, J.F.; Lima, C.; Borza, P.N. Smart grid security issues. In Proceedings of the 2015 9th International Conference on Compatibility and Power Electronics (CPE), Lisbon, Portugal, 24–26 June 2015; pp. 534–538.
41. Samie, F.; Bauer, L.; Henkel, J. Edge computing for smart grid: An overview on architectures and solutions. In *IoT for Smart Grids*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 21–42.
42. Data Captured by IoT Connections to Top 1.6 Zettabytes in 2020, As Analytics Evolve from Cloud to Edge. 2015. Available online: https://www.abiresearch.com/press/data-captured-by-iot-connections-to-top-16-zettaby/ (accessed on 9 April 2015).