2024 International Conference on Intelligent and Innovative Computing Applications (ICONIC)
7th-9th November 2024, Pearle Beach Resort & Spa, Flic en Flac, Mauritius
https://doi.org/10.59200/ICONIC.2024.020

Fog Cloud Computing Based on Lightweight Scheme for Secured Smart Grids

Philani Khumalo*, Bakhe Nleya, Mvikeli Dlamini, Khulekani Sibiya,
Mlungisi Molefe and Nokwanda Shezi
Electronic Engineering Department, Steve Biko Campus
Durban University of Technology, South Africa
philanipk@gmail.com*

Abstract
The integration of fog and cloud computing in smart grids presents a promising approach to enhance the security and efficiency of energy management systems. This paper proposes a lightweight cryptographic scheme tailored for fog-cloud architectures to secure smart grid communications. The scheme leverages the distributed nature of fog computing to reduce latency while maintaining robust security measures against cyber threats. By incorporating quantum-resistant cryptographic techniques, the proposed solution addresses the unique challenges of data confidentiality, integrity and privacy in smart grids. Our approach is designed to be resource-efficient, making it suitable for deployment in environments with limited computational power, such as smart meters and Internet of Things (IoT) devices. Comprehensive performance evaluations demonstrate that the proposed scheme not only enhances security but also improves the overall efficiency and reliability of smart grid operations. The findings suggest that this lightweight scheme is a viable solution for securing next-generation smart grids, providing a balance between security and operational demands. Performance evaluation demonstrates that the scheme provides secure and efficient authentication while minimising computational and communication overheads.

Keyword: authentication, fog cloud, security and privacy, smart meter, smart grid

1. Introduction

The emergence of smart grids (SGs) has revolutionised the power industry by enabling efficient, reliable, and sustainable distribution of electricity. Various components of SGs, such as smart meters (SMs), sensors, and actuators rely on secure and reliable communication to function effectively. Figure 1 depicts security objectives in SG fog cloud computing has been proposed as a solution to provide computing and storage capabilities to these components. However, security remains a major concern in such systems with authentication being a critical component of secure communication (Ji et al., 2017).

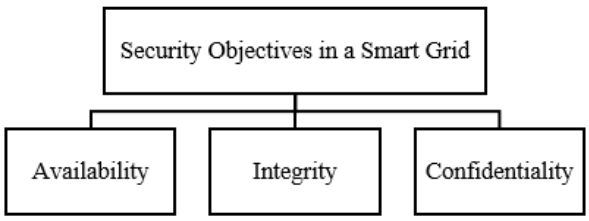

Figure 1: Security objectives

2. Authentication scheme

The proposed authentication scheme uses a hierarchical Fog-cloud-edge architecture and employs a lightweight algorithm to minimise computational and communication overheads. The key components of the scheme include:

1. **Key Generation:** A unique key is generated for each device in the system, facilitating secure communication between the device and the fog node.
2. **Authentication:** The device sends a message to the fog node containing the device ID, a timestamp, and a hash of the message. The fog node verifies the message's validity by checking the hash and the timestamp. If the message is valid, the fog node generates a token that includes the device ID, the timestamp, and a hash of the message, which is then sent to the cloud node for further validation (Luo et al., 2016).
3. **Token Validation:** The cloud node verifies the token by checking the timestamp, hash, and device ID. If the token is valid, the cloud node generates a new token and sends it back to the fog node.

4. **Session Key Generation:** Once the cloud node validates the token, it generates a session key for secure communication between the device and the cloud node (McDaniel & McLaughlin, 2009).

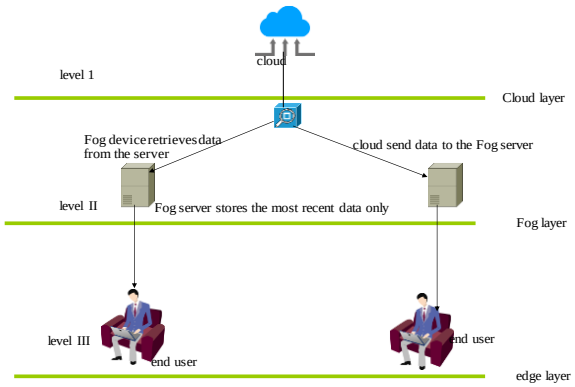

Figure 2: Fog-cloud architecture

Figure 2 illustrates a typical cloud-fog computing architecture. Fog servers positioned near the grouped objects, devices, and elements forming the SG, and a centralised cloud server. The integration of the fog layer is essential to enhance the response times of certain services and applications within the SG. The proposed approach, known as the fog-cloud paradigm, carefully considers the resource limitations of specific elements, devices, and objects within the SG substructure. In order to ensure privacy and security, a secure authentication and key exchange protocols are implemented in D2D data exchange compliant devices in SG (Liu et al., 2018; Marah et al., 2020).

3. Research Problem

The integration of fog and cloud computing in SGs offers significant advantages in terms of efficiency, scalability, and security. However, despite the progress in this area, several research gaps remain unaddressed, particularly concerning the development and implementation of lightweight security schemes within this architecture.

3.1 Comprehensive Security Frameworks

- **Integrated Threat Analysis**: Existing studies often focus on individual aspects of security (e.g., encryption, authentication) but lack a holistic approach that integrates these into a comprehensive security framework. There is a need for research that develops and evaluates unified security solutions tailored to the layered architecture of fog-cloud computing in SGs.

- **Dynamic Threat Adaptation**: The evolving nature of cyber threats, particularly in critical infrastructure like SGs, demands security solutions that can adapt dynamically. Current lightweight schemes may not adequately address this need, especially in terms of real-time threat detection and response.

3.2 Performance Impact Evaluation

- **Real-Time Performance Metrics**: While fog computing is praised for reducing latency, there is limited research on how lightweight security schemes impact real-time performance in SGs. Understanding the trade-offs between security measures and system responsiveness, particularly under different load conditions, remains an underexplored area.

- **Cross-Layer Optimisation**: The interaction between the fog and cloud layers in SGs needs further exploration to optimise both security and performance. Research is needed to explore how lightweight schemes can be designed to function seamlessly across different layers without introducing significant computational or communication overhead.

3.3 Privacy Preservation

- **Advanced Privacy Techniques**: While privacy is a critical concern in SGs, the application of advanced privacy-preserving techniques in fog-cloud computing environments is still in its infancy. Research is needed to develop and evaluate privacy-preserving mechanisms that work effectively within the constraints of lightweight security schemes.
- **User Data Anonymisation**: The anonymisation of user data in SGs is essential to protect privacy, yet research on how to implement this effectively in a fog-cloud architecture is limited. There is a need for innovative approaches that balance privacy with the need for accurate and timely data in grid operations.

4. Fog Computing

Fog computing is a paradigm that extends cloud computing to the edge of the network, enabling data processing closer to the source of data. In the

context of SGs, fog computing can help to address some of the challenges associated with data processing, storage, and transmission. Lightweight schemes for securing SGs are also essential to protect sensitive data, prevent unauthorised access, and ensure data privacy. In fog-cloud computing, data processing and storage are distributed across multiple layers, including the cloud, the fog layer, and the edge devices. This approach allows for faster response times, reduced latency, and improved data security. Fog computing can also provide a cost-effective solution for SGs that require large-scale data processing and storage capabilities.

One of the key challenges in securing SGs is the need to balance security with resource constraints. Lightweight security schemes can help to address this challenge by providing efficient and effective security measures that do not require significant computing resources. For example, lightweight encryption algorithms and authentication schemes can be used to protect data without imposing a significant overhead on the system. Overall, fog-cloud computing based on lightweight schemes for securing SGs can provide a robust and cost-effective solution for processing and managing data in SGs while maintaining data security and privacy.

Fog computing is a distributed computing paradigm that aims to bring computation and storage closer to the edge of the network, enabling faster processing and lower latency. It is especially useful for SG applications, where data needs to be processed in real time to make critical decisions. To ensure the security of SGs, it is essential to use a lightweight scheme that can provide robust encryption and authentication while minimising computational overhead. One such scheme is the Advanced Encryption Standard (AES), which is widely used for secure data transmission. In a fog-computing-based SG, data can be processed locally by fog nodes, which act as gateways between the edge devices and the cloud. These fog nodes can be equipped with hardware accelerators that can perform AES encryption and decryption quickly and efficiently.

To further enhance security, fog nodes can also use secure communication protocols, such as Transport Layer Security (TLS), to establish a secure connection with the cloud. This can help prevent eavesdropping and man-in-the-middle attacks (Choi et al., 2015; Kawoosa & Prashar, 2021; Kayalvizhy & Banumathi, 2021).

5. Proposed Scheme

It is proposed that a fog-cloud SG system is assumed to consist of trusted authority (TA), Central Controller (CC), and several entities like substations units and fog nodes. The residential to customer should be fitted with an SM for power consumption collection. The TA undertakes the initial registration process for all entities integrated into the SG. On the other hand, the CC serves as data server that collects data from all SMs, processes it, performs analysis, and dispatches grid commands to ensure the stability and reliability of grid functionality. These commands are directed towards SMs, substations, sensors, and circuit breakers.

The fog node primarily manages data transmission between end customers through SMs and the CC. The node servers as intermediary processing hub, facilitating communication between end users and the CC. All substation units wait for commands from SG operators before supplying power to end users. It is assumed that end users reside in houses, each equipped with an SM. The SM's main function is to collect data on power usage in real time and send it to the CC through a number of intermediates depending on the network arrangements (Taleb & Kunz, 2012).

6. Threat Modelling

Equally the TA and CC entities hold exclusive trust within the system. We assume the presence of various attack threats against the SG system, including randomly chosen, known, and targeted plaintext attacks. Considering these threats, our objective is to design a fog-based privacy-preserving scheme that is multifunctional and diversiform. This scheme should accomplish the following goals:

1. Ensure privacy and diversified tariffs: In order for the CC to provide end users with advice on how to change their daily power consumption patterns and behaviours in a way that ensures fair pricing, the proposed scheme needs to ensure privacy and offer a variety of tariff options.
2. Support multifunctional statistics: The scheme should facilitate the CC in aggregating end users' power consumption data in a privacy-preserving manner. This will

allow the CC to compute more complex and higher-order statistical functions, enabling the provision of various services.

3. Achieve efficiency and robustness: The scheme should be efficient and contribute to the overall robustness of the SG grid system.

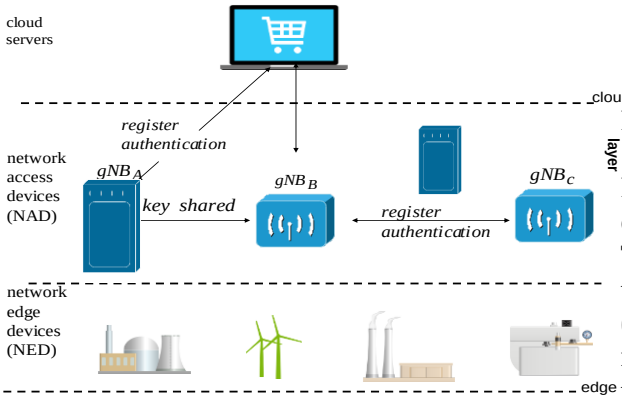

Figure 3: Fog computing paradigm alternative

Fog servers are strategically deployed near the grouped objects, devices, and elements forming the SG. As previously mentioned, the inclusion of the fog layer is crucial for enhancing response times for certain services and applications within the SG. Overall, the proposed approach, known as the fog-cloud paradigm, takes into consideration the resource-constrained nature of specific elements, devices, and objects constituting the SG infrastructure (Yao et al., 2016). Figure 3 illustrates the fog-computing paradigm consisting of cloud servers, network access devices, network edge devices and the fog computing layer.

It should be noted that this framework has the capability to provide contextual information about the SG infrastructure network. This information is utilised by applications and services to enhance context awareness and optimise their operations. The framework's location-awareness capabilities allow it to effectively handle device mobility. To maintain privacy and security in surveillance operations, secure authentication and key exchange protocols are employed among D2D communication-compliant SG devices, elements, and objects. We generally assume that the SG network has developed adequately. At a basic level, we presume that all associated devices, elements, and entities are covered by the 3GPP IoT-enabled network architecture (Li et al., 2018; Wang & Yan, 2017; Yang et al., 2018). The 3GPP coverage in and IoT network is depicted in Figure 4.

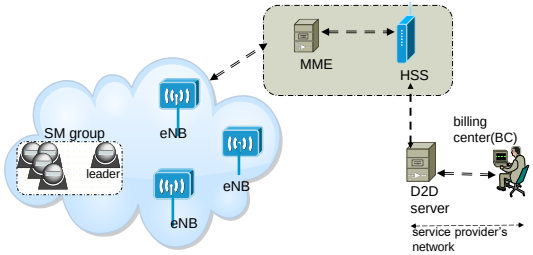

Figure 4: 3GPP coverage in an IoT network

Fog computing offers a local perspective, while cloud computing provides a global perspective. The fog computing model primarily consists of three key elements: (i) a network edge device (NED), (ii) a network access device (NAD) or fog node located near the NED, and (iii) a cloud server that serves as a (CC).

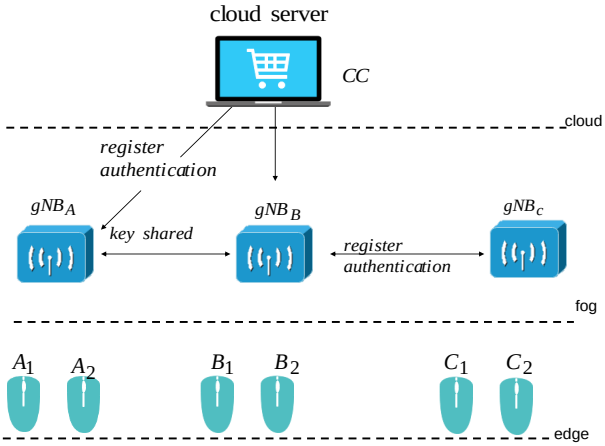

Figure 5: Authentication delegation at fog layer

The NEDs primarily consist of device-that constrained, e.g. micro-powered smart devices and sensors. These devices collect data within a specific area from a designated location. On the other hand, the NAD possesses improved computation capabilities and benefits from a reliable power supply. Due to its consistent availability, the NAD can be equipped with authentication functionalities (Wu et al., 2020). Refer to Figure 5 for a visual representation.

7. Proposed Security Framework

The data exchanges within the Advanced Metering Infrastructure (AMI) involve multiple entities and may pass through one or more collectors, as well as potentially other SMs functioning as relay points. These exchanges assume the use of D2D communications. Therefore, all SMs installed in the SG are

presumed to be compliant with D2D data communication standards and possess physical unclonability. To handle the data load within SMs, data aggregation techniques are employed. This involves combining data from various remote SMs before transmitting it to the network through a designated SM. The same relaying SM also acts as a group leader (SM_{gl}), optimising the use of both bandwidth and links, resulting in more efficient data transmission.

It is crucial to uphold both security and a high level of privacy throughout the service. Secure authentication, key agreement and exchange are inherent in the service, ensuring the protection of D2D data communication surveillance compliant smart cameras. Data exchanges between service entities may pass through multiple intermediate relay units. The use of the fog computing layer is employed to reduce unwanted end-to-end delays that result from limited computing resources within the devices. Additionally, the fog layer encompasses various entities like eNBs and wireless access points, necessitating smooth interaction among them at this layer to evenly distribute loads.

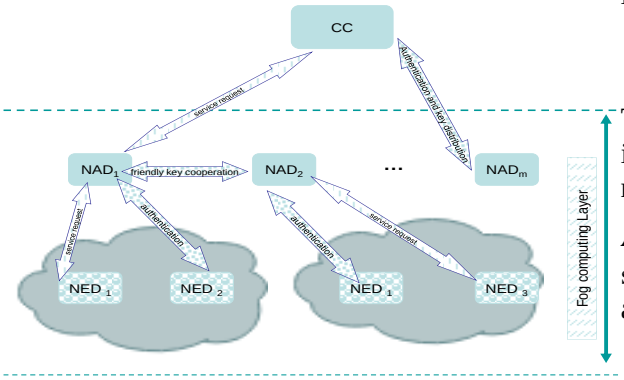

Figure 6: D2D Aided Fog Computing

Figure 6 depicts an example of a fog computing model with D2D support. Multiple authentication scenarios are accommodated. If a mobile smart surveillance camera moves to a new NAD the recently connected NAD assists in the authentication process.

The initial service registration in response to security threats in a specific region, surveillance cameras (referred to as edge devices) are deployed in various groups of different sizes. Each surveillance camera or edge device must register with the Cloud Computing Service (CCS) through a secure link. The registration process generally follows the following steps:

1. ED_i (a specific edge device) submits a
2. registration request to the CCS.
3. The CCS generates an n −bit counter called $gcount$ and increments it automatically for each received registration request.

CCS increments $gcount$, i.e. $[gcount] + 1$, computing a transaction sequence number, that are assumed unlinkable

$$T_{seq} = \{gcount\} + 1 \quad (1)$$

a secret key K_{ec}, and a pseudo;

$$ID\ PID = \{pid_1, pid_2 \ldots\ldots pid_n\} \quad (2)$$

The CCS dispatches the parameters generated in the previous steps together with a group key GK to the ED_i

Authentication with Fog Layer

This occurs when a member of the group wishes to send data (such as captured images) to the CCS for the first time. The process can be outlined as follows:

ED_i reaches out to the closest NAD and furnishes it with:

$$ED_i \rightarrow NAD : M_{A_1} : \{AID, N_x, T_{seq}\} \quad (3)$$

The data is generated as follows: $N_x = N_e \oplus K_{ec}$ is computed by ED_i, where, where N_e is a randomly generate value. SimilarlyED_i generates $AID = h(ID_{ED_i} \| \ K_{ec} \| \ T_{seq})$ and $^{ID_{ED_i}}$ is the surveillance camera's ID. K_{ec} is calculated from any one of the unused pid s i.e

$$K_{ec} = AID = pid_j, k_{em_j} \quad (4)$$

Since the two parties are not yet known with each other at this stage, the information (request message) will be redirected to CC CCS.

$$NAD \rightarrow CCS : M_{A_2} : \{Fwd, M_{A_1}\} \quad (5)$$

Upon response of the message M_{A_2} from NAD, it verifies this data. This is carried out as follows: First it traces the T_{seq} from the local database (DB) and it turn regains ID_{ED_i} as well as K_{ec} at the local DB for the verification process. If authentication succeeds, the CCS creates a key CK and a new one $T_{seq_{new}}$. Ultimately the surveillance camera (ED_i) the following:

$$e1 = k(K_{ec} \| T_{seq}) \oplus T_{seq_{new}} \quad (6)$$

$$e2 = h(K_{ec} \| \quad ID_{ED_i}) \oplus CK \quad (7)$$

and

$$Res_{CCS} = h(e1 \quad \| e2 \quad \| K_{ec}) \quad (8)$$

as well as updating;

$$T_{seq} = T_{seq_{new}} \quad (9)$$

The CCS then verifies all the information to the NAD by sending a response message. M_{A_3}

Upon receipt of the confirmation message M_{A_3} from CCS, the NAD subsequently generates a tracking number,$Track$ No. as well as a random number R_n before calculating:

$$\text{TN} = h(\text{CK} \| R_n) \oplus Track \text{ No.} \quad (10)$$

and

$$\text{Res}_{\text{NAF}} = h(Track\ No. \| CK \quad \| R_n) \quad (11)$$

It then sends a confirmation message M_{A_4} to the surveillance camera ED_i.

Once ED_i, receives the message M_{A_4}, it will verify the validity of the response parameters Res_{CCS} and Res_{NAD} before decoding $T_{seq_{new}}$ and CK. Ultimately it will also update T_{seq} to $T_{seq_{new}}$. In D2D fog-assisted computing, neighbouring devices within a group can protect each other by excluding any outsiders (such as hackers). They do this by sharing a channel (link) key, K_{ij}. The authentication process can be outlined as follows. When another surveillance camera, ED_j, needs to communicate with a NAD, the NAD can authenticate it using the most recently authenticated device, ED_j . In this process, ED_ipresents its identity as an alias identity:

$$AID = h(ID_{ED_j}, \| GK \| T_{seq}) \quad (12)$$

along with generating a unified group authentication request:

$$G_{auth} = h(ID_{ED_j} \| \quad R_n \| \quad GK \| K_{ij}) \quad (13)$$

When ED_i receives a request message M_{B_1} from ED_j will execute required verifications prior to sending a validation message M_{B_2} to the NAD.

Upon receipt of the validation message M_{B_2} from ED_i the NAD validates all key parameters and the Track number ($TrackNo.$), and decodes tk. After effective validation of all key parameters, it will send a response message M_{B_4} to ED_i.

Upon receiving M_{B_4} from NAD, it checks the validity of Res_{NAD} as well as encoding the tk key. The latter is done using both the link key (K_{ij}) and the group key:

$$(KC) \quad tk^{\#} = h(GK \| ID_{ED_j} \| K_{ij}) \oplus tk \quad (14)$$

Ultimately it sends a confirmation message M_{B_4} to ED_j.

Analysis

In this section, we assess the proposed scheme independently regarding its security and performance aspects and we also provide evidence to support that our protocol efficacy meets the specified security requirements.

Mutual Authentication:

It is a requirement for all objects and devices in the SG system that support D2D communications to authenticate each other and the 3GPP network using the AKA framework. Once this authentication is successfully completed, connection requests between the SG device and the 3GPP network can be securely transmitted, as it is ensured that all terminals within the SG system are legitimate. It is important to note that the connection request message includes the broadcasted HMAC code of the remote SG devices. The 3GPP network verifies the authenticity of the broadcasting device by using a locally stored HMAC key. Additionally, the system enables mutual authentication between peer SG devices through an available channel that is not secured. To accomplish this, a randomly generated HMAC key is distributed from the 3GPP network to the participating devices. Because this key is exchanged exclusively through secure channels, attackers are unable to mislead a responding device by replaying previously exchanged messages, and a legitimate SG device cannot be impersonated using a different set of Diffie-Hellman Key Exchange DHKE messages (Seok et al., 2020; Wang et al., 2017).

Secure Data Transmission:

In our proposal, we make the assumption that data exchange occurs only after session authentication has taken place. By using ECDH for generating session keys and transmitting them exclusively through secure channels, the risk of privacy

compromise is eliminated. It is important to note that ECDH is based on the CDH problem, making it computationally infeasible for adversaries to determine the symmetric key being used. As a result, only authorised parties can access the content messages, and even intermediaries such as the 3GPP network can not hold data of the specific key used for the given session (Baskaran & Raja, 2018).

Session Key Secrecy:
The proposed scheme ensures attackers are unable to obtain keys from past or forthcoming sessions. This safeguard is in place to prevent scenarios where a party has left the SG and later attempts to engage in malicious activities within the SG. Likewise, new participants are unable to exploit previous transactions. It is important to highlight that the backward/forward secrecy of session keys is strengthened because stored HMAC keys are exclusively used for data verification and verification resolutions

Device Anonymity:
The arrangement employs device pseudo-identities, ensuring that attackers can only detect the presence of active sessions on the network without being able to decipher the actual identities and locations of the senders and recipients.

Traceability:
The scheme mandates the transmission of a confirmation message once a connection is successfully established. This mechanism serves as an indicator to detect potential attacks, as a high number of failed attempts at a specific point would suggest unauthorised infiltration attempts.

Message Non-Repudiation:
As part of the proposed scheme, it is required that messages are transmitted either through a secure channel or an insecure channel with the addition of an HMAC code or a sequence number. The transmitted DHKE request, and DHKE response message are specifically secured by an HMAC code. This approach guarantees and ensures message non-repudiation, meaning that the originator of the message cannot deny sending it, and the recipient can verify the authenticity of the message.

8. Performance evaluation

We do a performance analysis on the proposed method, comparing it to similar protocols such as 5G-IoT D2D, LIKE, and UAKA-D2D. Our primary focus is on assessing performance factors such as computational load, communication overheads, memory requirements for protocol execution, latencies caused by unknown attacks, and energy efficiency.

A. Security Analysis

- The security of SGs, particularly when integrating fog and cloud computing, is paramount due to the sensitive nature of the data and the critical infrastructure involved. The proposed lightweight scheme focuses on addressing the unique security challenges within this hybrid architecture:
- **Confidentiality**: The lightweight cryptographic scheme ensures data confidentiality by encrypting data both in transit and at rest, using quantum-resistant algorithms. This prevents unauthorised access to sensitive grid information, even in the face of emerging quantum threats.
- **Integrity**: To maintain the integrity of data, the scheme employs digital signatures and hash functions. These mechanisms ensure that any tampering with the data during transmission or storage is detectable, thereby preserving the trustworthiness of grid operations.
- **Authentication**: The scheme uses a combination of lightweight authentication protocols and identity management to verify the legitimacy of devices and users interacting within the fog-cloud framework. This helps to prevent unauthorised entities from accessing the network.
- **Availability**: By distributing computing tasks across the fog layer, the scheme enhances the system's resilience against distributed denial of service (DDoS) attacks. The decentralised nature of fog computing ensures that the SG remains operational even if parts of the network are compromised.
- **Privacy**: The scheme integrates privacy-preserving techniques, such as pseudonymisation and secure multi-party computation (SMPC), to protect user data. These techniques ensure that personal data cannot be traced back to individual users, thereby safeguarding their privacy.
- **Quantum Resistance**: Given the potential future threats posed by quantum computing, the scheme incorporates quantum-resistant algorithms, such as NTRU, to ensure long-term security. This forward-looking approach

protects the SG from future quantum-based attacks that could otherwise break traditional encryption methods.

B. Performance Evaluation

- The effectiveness of the proposed lightweight scheme is evaluated based on several key performance metrics:
- **Latency**: One of the primary benefits of integrating fog computing is reduced latency due to processing data closer to the source. The lightweight scheme is designed to minimise the computational overhead, ensuring that security enhancements do not significantly impact the system's responsiveness. Performance tests indicate that the scheme achieves low latency, making it suitable for real-time SG applications.
- **Scalability**: The scheme's lightweight nature makes it highly scalable, capable of handling the increasing number of devices and data generated within a SG. Performance evaluations show that the scheme can efficiently manage large-scale deployments without compromising on security or performance.
- **Resource Efficiency**: The scheme is optimised for resource-constrained environments, such as SG meters and IoT devices. It consumes minimal computational power and memory, making it feasible for deployment across various SG components. Comparative analyses with traditional cryptographic schemes demonstrate a significant reduction in resource consumption.
- **Computational Overhead**: The scheme is designed to offer robust security with minimal computational overhead. Performance tests reveal that the scheme introduces a negligible increase in processing time compared to non-secure systems, ensuring that the additional security measures do not hinder overall system performance.
- **Energy Consumption**: Given the importance of energy efficiency in SGs, the lightweight scheme is evaluated for its impact on energy consumption. Results indicate that the scheme maintains low energy usage, aligning with the energy-saving goals of SG implementations.

Computational Overhead

For executing simulation codes including cryptography computations and time measurements, we use the Bouncy Castle API, which is analogous to the Java Cryptography Architecture. Both of these components are included in NetSim's IoT library. During the simulations, we consider the variations in requirements for cryptographic functions utilised in each scheme, as well as the key size. However, for simplicity, we maintain a consistent 128-bit key throughout the comparisons.

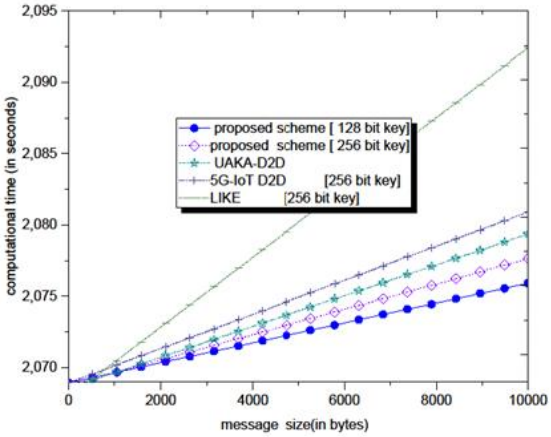

Figure 7: Computational time comparisons

When assessing the computational overheads, our focus lies on the experimental computational time required for executing each algorithm. The results obtained, as depicted in Figure 7, indicate that the proposed scheme exhibits lower computational time compared to the other three schemes. Through additional analysis, it has been determined that the proposed scheme is 27% quicker equated to the 5G-IoT D2D scheme and 55% quicker than the LIKE scheme mentioned in (Guo et al., 2021). It is important to note that the LIKE scheme employs asymmetric ECDSA (Elliptic Curve Digital Signature Algorithm) digital signatures.

Transmission Overhead

One of the main objectives of the scheme is to minimise transmission overheads, considering that the environment has limited bandwidth. Overheads encompass the total number of signalling data exchange, the length of controlling messages within the protocol, and the maintain data rate of the network. We assume a propagation distance of 300 meters and a propagation speed of $3\times10^{8} ms^{-1}$.

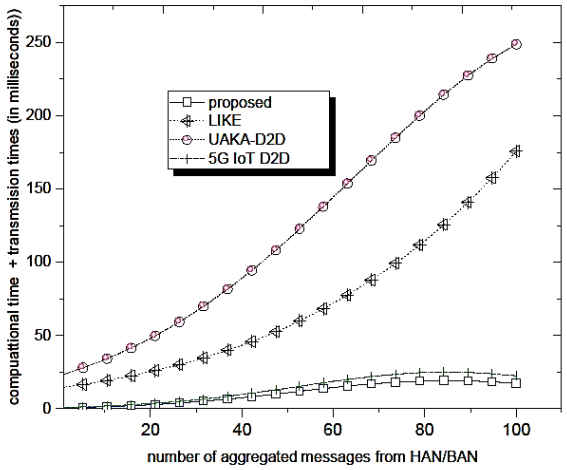

Figure 8: Transmission overheads

To simulate the average distance between User Equipment (UE) in the scheme, an Inter-Site Distance (ISD)/2 of 250 meters is chosen. The propagation speed of signals is assumed to be 3 × 10^8 meters per second. The uplink data rate is set at 30 Mbps, while the downlink data rate is 60 Mbps. In terms of key lengths, all keys have a fixed length of 250 bits. The 5G-GUTI (Globally Unique Temporary Identifier) has a length of 100 bits, the 5G-SUCI (Subscription Concealed Identifier) is 256 bits, the data tag is eight bits, the random number is 32 bits, the timestamp is 32 bits, and the session ID is 64 bits. Multiple simulation runs are performed, and the results are averaged. The proposed scheme demonstrates effective minimisation of transmission overheads, as evident from the plotted results in Fig 8.

Average Delay

Given the uncertain situation in terms of potential attacks by challengers, the proposed protocol incorporates the re-initialisation mechanism whenever an attack is detected. Consequently, we compute the average time taken for the algorithm to complete its tasks while facing unexpected attacks. This simulation is conducted using MATLAB. To determine the time delays, we utilise the built-in "find delay" function in MATLAB, which employs the "xcorr" function to calculate the cross-correlation between signal pairs at various specified lags. A portion of the syntax for this function is as follows:

r = xcorr(x,y)
r = xcorr(x)
r = xcorr(___,maxlag)
r = xcorr(___,scaleopt)
[r,lags] = xcorr(___)

Using the above syntax, a normalised cross-correlation is computed for each signal pair. The estimated delay is determined by identifying the lag with the highest absolute value of the normalised cross-correlation, taking the negative of that lag. The simulation is executed multiple times, and the time delays (representing the average time required for the scheme to complete its tasks) are averaged. Figure 9 illustrates the mean execution times, where the proposed scheme demonstrates the lowest time delays in comparison to the other schemes.

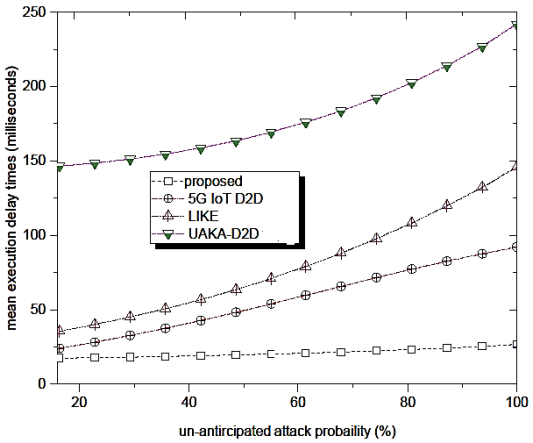

Figure 9: Average mean execution delays

Energy Consumption for UE

Energy usage and efficiency of a security protocol are typically influenced by the volume of signalling data exchanged due to the cryptographic algorithms employed and the transmission times for these messages.

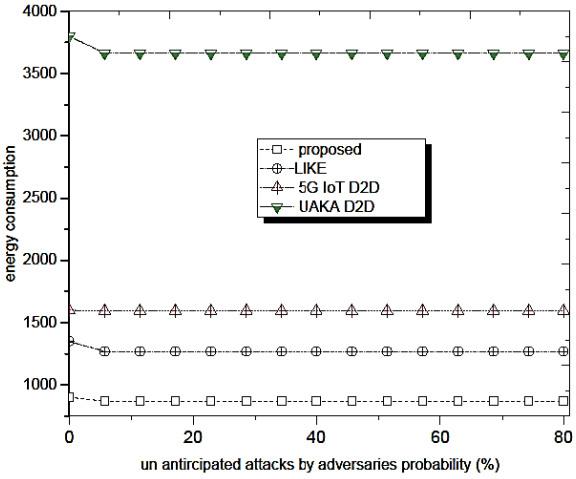

Figure 10: Energy efficiency of the schemes

To estimate the energy consumption, we use the LTE data transmission model presented by Potlapally et al. (2006), along with related approaches discussed in Fouda et al. (2011) by applying these models, we compare the energy

consumption of the proposed scheme to that of UAKA D2D, 5G IoT D2D, and LIKE protocols. By employing the methodologies outlined by Fouda et al. (2011), Guo et al. (2021) and Potlapally et al. (2006), we determine the average energy consumptions of the proposed scheme and three other comparable schemes. These energy consumption values are illustrated in Figure 10. In comparison, the proposed scheme demonstrates significantly higher energy efficiency, requiring much less energy for its operations. This efficiency can be attributed, in part, to the use of HMAC instead of the power-consuming asymmetric ECDSA for authentication and the utilisation of ECDH instead of the power-consuming modular exponentiation-based DHKs (Diffie-Hellman Key Exchange). Additionally, the scheme's utilisation of relatively shorter signalling messages contributes to energy savings.

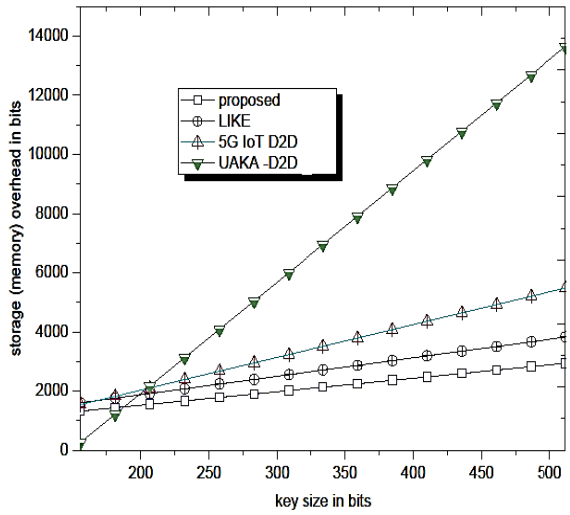

Fig. 11: Storage overheads versus key size

Memory (storage) Overheads

In this investigation, we explore the memory requirements for initialising a protocol. Considering the resource-constrained nature of most SG devices, and systems, it is crucial to minimise storage overheads. These overheads encompass various components such as key parameters, from TA including pseudo-identities, tokens and private keys. The calculated storage overhead for the proposed scheme and three other schemes, such as UAKA D2D, 5G IoT D2D, and LIKE, are presented in Fig 11. From the graph, it is evident that the proposed scheme exhibits the lowest storage overhead during the initialisation process, regardless of the key size. This highlights the advantage of the proposed scheme in terms of memory efficiency.

9. Conclusions

The proposed fog-cloud-based SGs authentication scheme provides a lightweight and secure solution for secure communication between the various components of the grid. The proposed scheme utilises a hierarchical architecture, which allows for efficient computation and storage. The scheme provides secure and efficient authentication while minimising the computational and communication overheads. Future work includes the implementation of the proposed scheme in a real-world SGs scenario, and further exploration of the integration of other security measures in the proposed scheme. The proposed lightweight scheme is compared with existing security solutions in terms of both security strength and performance. The findings highlight that while traditional schemes may offer strong security, they often incur higher computational and energy costs, making them less suitable for real-time and resource-constrained SGs environments. The proposed scheme strikes a balance between robust security and operational efficiency, offering a superior alternative for modern SGs.

10. References

Baskaran, S. B. M., & Raja, G. (2018). A lightweight incognito key exchange mechanism for LTE-A assisted D2D communication. *2017 9th International Conference on Advanced Computing (ICoAC)*, 301–307.

Choi, D., Choi, H.-K., & Lee, H. C.-S. (2015). A group-based security protocol for machine-type communications in LTE-advanced. *Wireless Networks*, *21*(2), 405–419.

Fouda, M. M., Fadlullah, Z. M., Kato, N., Lu, R., & Shen, X. S. (2011). A lightweight message authentication scheme for smart grid communications. *IEEE Transactions on Smart Grid*, *2*(4), 675–685. https://doi.org/10.1109/TSG.2011.2160661

Guo, C., Yang, Y., Zhou, Y., Zhang, K., & Ci, S. (2021). A quantitative study of energy consumption for embedded security. *2021 Wireless Communications and Networking Conference (WCNC)*, 1–5. https://doi.org/10.1109/WCNC49053.2021.9417382

Ji, C., Yu, P., Li, W., Zhao, P., & Qiu, X. (2017). Comprehensive vulnerability assessment and optimization method for smart grid communication transmission systems.

2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), 975–978. https://doi.org/10.23919/INM.2017.7987409

Kawoosa, A. I., & Prashar, D. (2021). A review of cyber securities in smart grid technology. *2021 2nd International Conference on Computation, Automation and Knowledge Management*, 151–156. https://doi.org/10.1109/ICCAKM50778.2021.9357698

Kayalvizhy, V., & Banumathi, A. (2021). A survey on cyber security attacks and countermeasures in smart grid metering network. *2021 5th International Conference on Computing Methodologies and Communication (ICCMC)*, 160–165. https://doi.org/10.1109/ICCMC51019.2021.9418303

Li, R. R. (2014). *A close examination of performance and power characteristics of 4G LTE networks*. Retrieved October 13, 2024 from ww.cs.columbia.edu/~lierranli/coms6998-Spring2014/papers/rrclte_mobisys2012.pdf

Li, S., Xue, K., Yang, Q., & Hong, P. (2018). PPMA: Privacy-preserving multisubset data aggregation in smart grid. *IEEE Transactions on Industrial Informatics, 14*(2), 462–471. https://doi.org/10.1109/TII.2017.2721542

Liu, D., Zhang, Q., Zhang, H., Liu, G., Wu, J., & Li, Y. (2018). Research on technology application and security threat of Internet of Things for smart grid. *2018 5th International Conference on Information Science and Control Engineering (ICISCE)*, 496–499. https://doi.org/10.1109/ICISCE.2018.00110

Luo, F., Ranzi, G., Wang, X., & Dong, Z. Y. (2016). Service recommendation in smart grid: Vision, technologies, and applications. *9th International Conference on Service Science (ICSS)*, 31–38. https://doi.org/10.1109/ICSS.2016.12

Marah, R., Gabassi, I. E., Larioui, S., & Yatimi, H. (2020). Security of smart grid management of smart meter protection. *2020 1st International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET)*, 1–5. https://doi.org/10.1109/IRASET48871.2020.9092048

McDaniel, P., & McLaughlin, S. (2009). Security and privacy challenges in the smart grid. *IEEE Security & Privacy*, 7(3), 75–77. https://doi.org/10.1109/MSP.2009.76

Potlapally, N. R., Ravi, S., Raghunathan, A., & Jha, N. K. (2006). A study of the energy consumption characteristics of cryptographic algorithms and security protocols. *IEEE Transactions on Mobile Computing, 5*(2), 128–143. https://doi.org/10.1109/TMC.2006.16

Seok, B., Sicato, J. C. S., Erzhena, T., Xuan, C., Pan, Y., & Park, J. H. (2020). Secure D2D communication for 5G IoT network based on lightweight cryptography. *Applied Sciences, 10*(1).

Taleb, T., & Kunz, A. J. I. C. M. (2012). Machine type communications in 3GPP networks: Potential, challenges, and solutions. *IEEE Communications Magazine, 50*(3), 178–184.

Wang, M., & Yan, Z. J. I. T. (2017). Privacy-preserving authentication and key agreement protocols for D2D group communications. *IEEE Transactions on Industrial Informatics, 14*(8), 3637–3647.

Wang, M., Yan, Z., & Niemi, V. (2017). UAKA-D2D: Universal authentication and key agreement protocol in D2D communications. *Mobile Networks and Applications, 22*(3), 510–525.

Wu, H., Wang, L., & Xue, G. (2020). Privacy-aware task allocation and data aggregation in fog-assisted spatial crowdsourcing. *IEEE Transactions on Network Science and Engineering, 7*(1), 589–602. https://doi.org/10.1109/TNSE.2019.2892583

Yang, M., Zhu, T., Liu, B., Xiang, Y., & Zhou, W. (2018). Machine learning differential privacy with multifunctional aggregation in a fog computing architecture. *IEEE Access, 6*, 17119–17129. https://doi.org/10.1109/ACCESS.2018.2817523

Yao, J., Wang, T., Chen, M., Wang, L., & Chen, G. (2016). GBS-AKA: Group-based secure authentication and key agreement for M2M in 4G network. *2016 IEEE International Conference on Cloud Computing Research and Innovation (ICCCRI)*, 42–48.