mathematics

MDPI

Article

Development of a Lightweight Centralized Authentication Mechanism for the Internet of Things Driven by Fog

Jan Lansky [1], Mahyar Sadrishojaei [2], Amir Masoud Rahmani [3,*], Mazhar Hussain Malik [4], Faeze Kazemian [5] and Mehdi Hosseinzadeh [6,*]

[1] Department of Computer Science and Mathematics, Faculty of Economic Studies, University of Finance and Administration, 10100 Prague, Czech Republic
[2] Faculty of Industry, University of Applied Science and Technology (UAST), Tehran 11369, Iran
[3] Future Technology Research Center, National Yunlin University of Science and Technology, Douliou 64002, Taiwan
[4] Department of Computer Science and Creative Technologies, University of the West of England—UWE Bristol, Bristol BS16 1QY, UK
[5] Department of Computer Science, University of Applied Science and Technology (UAST), Tehran 11369, Iran
[6] Pattern Recognition and Machine Learning Lab, Gachon University, 1342 Seongnamdaero, Seongnam 13120, Korea
* Correspondence: rahmania@yuntech.edu.tw (A.M.R.); mehdi@gachon.ac.kr (M.H.)

Abstract: The rapid development of technology has made the Internet of Things an integral element of modern society. Modern Internet of Things' implementations often use Fog computing, an offshoot of the Cloud computing that offers localized processing power at the network's periphery. The Internet of Things serves as the inspiration for the decentralized solution known as Fog computing. Features such as distributed computing, low latency, location awareness, on-premise installation, and support for heterogeneous hardware are all facilitated by Fog computing. End-to-end security in the Internet of Things is challenging due to the wide variety of use cases and the disparate resource availability of participating entities. Due to their limited resources, it is out of the question to use complex cryptographic algorithms for this class of devices. All Internet of Things devices, even those connected to servers online, have constrained resources such as power and processing speed, so they would rather not deal with strict security measures. This paper initially examines distributed Fog computing and creates a new authentication framework to support the Internet of Things environment. The following authentication architecture is recommended for various Internet of Things applications, such as healthcare systems, transportation systems, smart buildings, smart energy, etc. The total effectiveness of the method is measured by considering factors such as the cost of communication and the storage overhead incurred by the offered integrated authentication protocol. It has been proven that the proposed technique will reduce communication costs by at least 11%.

Keywords: Internet of things; mutual authentication; fog; cloud computing; key agreement; asymmetric key

MSC: 68M18

Citation: Lansky, J.; Sadrishojaei, M.; Rahmani, A.M.; Malik, M.H.; Kazemian, F.; Hosseinzadeh, M. Development of a Lightweight Centralized Authentication Mechanism for the Internet of Things Driven by Fog. *Mathematics* **2022**, *10*, 4166. https://doi.org/10.3390/math10224166

Academic Editor: Daniel-Ioan Curiac

Received: 3 October 2022
Accepted: 1 November 2022
Published: 8 November 2022

1. Introduction

The Internet of Things (IoT) allows the integration of numerous nodes and objects that may connect directly without human involvement [1]. Physical devices, including nodes, which track and collect information from equipment to human social interactions, are included among the Internet of Things [2]. In the IoT era, everything in the lives of humans can be constantly connected to everything else [3]. Connecting everyday objects, such as refrigerators, microwaves, dishwashers, and other kitchen appliances, is one of the most

important goals of the IoT, which aims to build a network infrastructure with open and adaptable communication protocols and applications [4]. The IoT has acquired universal support in the last few decades in the fields of network infrastructure, medicine, business services, and even e-learning. Unfortunately, the need for multiple implementations of the IoT has been quickly expanding, leading to a severe security risk [5,6].

Cloud technology has opened up many possibilities for users over the last century, by providing them with diverse solutions [7]. It has become more practical to employ Cloud services models instead of purchasing and administering private data centers for users dealing with online apps and file management [8]. Utilizing Cloud services liberates end-users from defining numerous details, including storage capacity, computer limitations, and network connection costs [9]. On the other hand, latency-sensitive apps need nodes in immediate proximity to one another to achieve their timing constraints, making this latency an issue [10]. While IoT methods and gadgets have become more integrated into people's lives, with billions of these objects gaining more capabilities, the present Cloud computing systems cannot meet their criteria for mobility support, location-based services, and reduced latency [11,12].

The Fog is a layer that sits among users and the Cloud, allowing Cloud servers located far away in cyberspace to be brought closer to the edge and become available over a more extensive range [13,14]. End devices, including access points, could be used to host services in the Fog computing environment, as demonstrated in Figure 1. This innovative multi-layered distributed computing environment enables apps to run as near as possible to the detected, relevant, and enormous data flowing from persons, processes, and things, while maintaining high performance [15,16]. Data, computing, storing, and application facilities are available at the edge for both Cloud and Fog technologies [17,18]. On the other hand, Fog could be separated from the Cloud because it is closer to end-users, has a dense geographic range, and allows for movement [19,20]. The Fog computing structure consists of three layers: the terminal layer, the Fog layer, and the Cloud layer. Figure 1 depicts the three-layer design and a thorough definition of Fog computing:

(1) **Edge layer:** This layer is nearest to users and devices and comprises numerous IoT or smart gadgets, including sensors, cell phones, smart cars, smart cards, and readers. Even though gadgets are capable of computation, they are often just used to perform the intelligent sensing of individual events or objects and to transmit the obtained information to the top layer for later storage and processing.

(2) **Fog layer:** This layer is situated at the network's edge and contains many Fog nodes. Typically, these Fog nodes comprise routers, gateways, switchers, access points, base stations, and Fog servers. These Fog nodes could be dispersed extensively among terminal devices and the Cloud, including at cafes, malls, subway stations, roads, and playgrounds. Smart services can be provided via Fog nodes located in a fixed location or on a vehicle connected to terminal devices. Furthermore, they may compute, transfer, and collect the sensed information they obtain, enabling fundamental analysis and delay-sensitive apps inside the Fog layer. In conclusion, Fog nodes are linked to IP core networks and Cloud data centers, and, by collaboration with Cloud data centers, they could acquire more robust storage and processing features.

(3) **Cloud layer:** The Cloud layer consists of several storage features and servers with superior efficiency, to offer a variety of innovative software solutions including connected homes, intelligent transportation, smart manufacturing, and competent healthcare. This layer offers robust storage and computation capabilities to facilitate a wide variety of computational analyses and store a considerable quantity of data. In contrast to the standard Cloud computing paradigm, Fog computing does not perform all computations and storage in the Cloud. Various management tactics may be used to efficiently handle and organize the core Cloud to increase the usage of Cloud resources, per the requirement load principle.

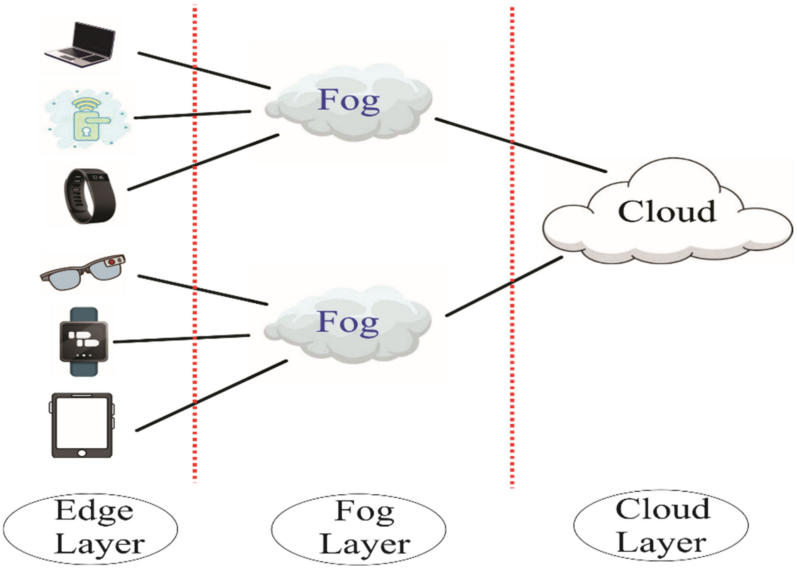

Figure 1. Structure of IoT ecosystem assisted by Fog.

In an IoT object network scenario, the client console collects input from the devices, such as sensitive personal information sensors, emphasizing the significance of authentication [21]. Various types of threats can occur on an IoT network, just as in other wireless transmission systems [22]. These include man-in-the-middle (MITM), replay, visualization, and transitory hidden leak attacks [23].

Even though the incorporation of IoT-based smart services into Fog computing has the possibility of playing a pivotal part in the delivery of a wide variety of smart application services to already-implemented smart devices more effectively, there are currently possible privacy and security dangers that must be avoided. First, the high frequency with which data is collected might pose significant threats to location privacy and make it easier for adversaries to monitor smart devices. In addition, the identity of Fog nodes and smart objects might be assumed by an attacker in order to unlawfully transfer malicious content or collect data in violation of the terms of service.

Numerous verification protocols have been proposed for the IoT; however, the vast majority of the current authentication protocols outlined do not operate well; many are not safe against authentication threats, some may not offer additional anonymity and tracking, and others are not light, according to the research [24]. In other words, these designs' communication and computation expenses are tremendous [25]. Due to this, it would be highly beneficial to have a lightweight authentication system for mutual authentication among IoT nodes and Cloud-based Fog services [26]. The proposed mechanism is a practical solution to supply proper authentication for the IoT. In general, the following contributions have been made:

- Overcoming certain shortcomings in the relevant literature;
- Exploring the infrastructure toward distributed Fog computing;
- Developing a lightweight authentication framework for mutual authentication;
- Utilizing lightweight, low-cost, and computationally straightforward encryption procedures;
- Creating a centralized authentication method by a Trusted Third Party (TTP) for mutual authentication;
- Investigating security threats, including eavesdropping, MITM, replay attack, side-channel, and brute force;
- Assessing the authentication scheme effectiveness.

The remaining paper progresses in four sections. The first discusses the research underlying the suggested strategy. The recommended authentication technique is explained

in great length in the Section 2. The Section 3 covers the security study and assessment of the authentication method. Ultimately, the article finishes with a summary of probable future initiatives.

2. Literature Review

Saleem and Ghaffar [27] have proposed a unique identity-based key agreement mechanism targeting mobile users in an IoT context that makes use of puncturable pseudorandom operations. Using the suggested technique, two moving users can perform mutual authentication with the help of a central server. The recommended strategy is subjected to formal and informal evaluation in order to identify the overall level of security. The random oracle concept, which is frequently used in security research, is used to illustrate the formal security assessment. This approach has the lowest transmission and computation overhead of all the protocols tested. One downside to this approach is that it does not allow post-quantum cryptography techniques.

Furthermore, Lee and Chen [28] have described a safe authentication mechanism for the Fog computing platform, which will include the compatibility of collaborative Device to Device (D2D) connectivity. Since the sensors' resources and power were also constrained, the proposed scheme makes use of lightweight encryption algorithms, such as a one-way hash algorithm called the Barrel Shifter Physically Unclonable Function (BS-PUF), to strengthen the safety of the sensors and Fog nodes, while minimizing the computational load on the gadgets. While the suggested algorithm is resistant to possible threats, it also supplies greater security and efficiency. Regrettably, this strategy performs poorly in a real-world setting.

Guo and Zhang [29] have designed a secured remote user authentication strategy that provides secure connection at the platform's edge and remote authentication in Fog-enabled intelligent home devices. The technique consists of the edge negotiation stage and the authentication stage. Furthermore, this protocol does not retain critical client and smart gadget information in the memories of the smart gateway, hence preventing numerous attacks that would be induced by a compromised gateway. This technique reduces computation and communication costs, while increasing security characteristics. However, this approach has a number of downsides, such as a longer-than-usual complexity and high execution time.

Iqbal and Bhola [30] have offered an Elliptic Curve Cryptography (ECC)-based secure key exchange mechanism for use by IoT objects and Fog coordinators in order to circumvent the constraints imposed by a Lightweight Secure Key Exchange (LKSE). Based on the cryptanalysis, it appears that LKSE is susceptible to threats involving spoofing and MITM. The Burrows–Abadi–Needham (BAN) logic and the random oracle theory were used to conduct an analysis that determined how secure the approach that was devised is. For the purpose of performing automatic security verification on the suggested method, simulations have been carried out using Automated Validation of Internet Security Protocols and Applications (AVISPA). However, one of the most major limitations is the issue of privacy.

Moreover, Verma and Bhardwaj [31] have planned a mutual authentication and key agreement technique, based on ECC, to facilitate safe D2D communication and Fog servers. ECC is short for elliptic curve cryptography. The approach given is secure against many assaults, based on the results of an informal security study of the scheme. The computing and storing overhead have been taken into consideration in the performance analysis that was done. One of the method's negative points is the unavailability of key distribution and a key generator for the security framework.

Li and Miao [32] have discussed a new protocol as a solution to the problems of being susceptible to internal assaults, theft attacks involving smart cards, and a lack of flawless forward security. Analyses of the security and performance of this protocol demonstrate that it completely overcomes these restrictions and demonstrates exceptional efficiency and performance. One limitation of this strategy is that it underperforms mutual authentication among low-power and processing machines.

In addition, Rana and Mishra [33] have presented a key agreement mechanism for the IoT ecosystem that Fog backs, in order to establish responsibility, while also protecting personal information. Both in terms of efficiency and security, the suggested approach performs admirably. As a result of the generally accepted random oracle model, it has demonstrated to be provably secure against every attacker with a probability distribution over polynomial time. Its disadvantages involve a high overload.

Shukla and Thakur [34] have suggested an innovative approach based on Fog computing and the blockchain, which was accepted. It consists of a three-tier infrastructure focusing on Fog computing, an analytical model, a mathematics structure, and an Advanced Signature-Based Encryption (ASE) technique for verifying and identifying IoT devices. The goal is to increase the amount of safe data transfer for IoT gadgets and end-users using real-time operations. The suggested architecture and method would be capable of providing safe transactions and communication operations at the edge of the network. It features a greater throughput, minor packet error, and better dependability than the previous algorithm. Low scalability is one of the technique's primary drawbacks.

Wu and Lee [35] have introduced a novel authentication key-exchange system that makes usage of Fog nodes for relaying nodes to increase security. When the technique completes mutual authentication, a session key is generated for future secure connections. In order to formally test the safety of the system, the automatic verification program ProVerif and BAN logic are employed. The informal study reveals that the plan is resistant to several well-known assaults. Unfortunately, the amount of memory required to run this method is considerable.

Soni and Singh [24] have established a lightweight, secure health authentication and key agreement that uses low-cost procedures. It is necessary to conduct an evaluation process against a wide variety of security assaults to validate the suggested method's resilience. According to the results of computational research, the recommended protocol has a significantly lower execution cost and substantially less computing time and power consumption. In addition, this mechanism has a lower communication overhead and a reduced storage cost. Unfortunately, this algorithm has poor reliability.

Hammi and Fayad [26] have devised an innovative One-Time Password (OTP) creation method to ensure IoT devices' security. This method makes use of ECC and isogeny. The efficiency of this technique is checked with a genuine construction, and its effectiveness is evaluated in two alternative ways, namely a time-based OTP and a hash message authentication code-based OTP. The acquired statistical results illustrate the effectiveness and efficiency of this strategy concerning performance and security. The negative aspects of it include a high overload and an extra degree of complexity.

Alqahtani and Al-Makhadmeh [25] have created a Trust-Based Monitoring (TBM) strategy to enhance Cloud-assisted IoT setups' safety. Such security architecture utilizes intelligent agents and middleware to manage user- and communication-level security. TBM consists of three steps of security administration: spoof detection, trust establishment, and message authentication. Intelligent agents are accountable for guaranteeing safe connections by communicating trust and signal strength measurements with the middleware. Additionally, such agents aid with tracking, analyzing, and task shifting to save connection expenses. The results indicate the system's consistency in reducing response and detection durations, misdetection probability, and false positive ratios. Furthermore, it was discovered that it increases the system's lifespan by reducing power use. The main disadvantage is its inefficient memory consumption.

Shahidinejad and Ghobaei-Arani [36] have described a lightweight authentication system for IoT devices, called Light-Edge. This method uses a three-tier architecture consisting of an IoT device layer, a trusted center only at the edge layer, and Cloud service providers. The proposed technique is better than other methods regarding its resilience to attacks, time, and communication cost. Sadly, this system has a critical flaw: information can leak out.

Abdussami and Amin [37] have advanced a lightweight, safe mutual authentication technique premised on a physically unclonable feature to solve these problems. Due to the limited resources of the Fog nodes, a simple authentication method is recommended. The random or real paradigm is used for the formal safety analysis of this system. The mentioned scheme has outstanding performance in computation and communication costs, and it is also resistant to a wide variety of attacks. However, this plan has a problem with getting out of synchronization.

Finally, Erroutbi and El Hanjri [38] have provided the background, characteristics, and essential differences between the Cloud platform and the Fog concept, as well as their impacts on the IoT, and have evaluated numerous Fog computing applications. Next, a mutual authentication approach built on a Hash-based Message Authentication Code (HMAC) is presented for defending IoT-enabled apps in the Fog. The method also details potential restrictions on its use and possible avenues for cyberattacks. This approach has some limitations, one of which is that it does not work well for mutual authentication between computers with low processing power and energy consumption.

The main strengths and weaknesses of the analyzed algorithms are laid forth in Table 1. Both the communication cost and the extra overhead of the aforementioned methods are significant drawbacks, especially given their importance to the IoT system. In addition to attempting to solve these problems, the proposed method also tackles serious and nuanced security concerns.

Table 1. Summary of the techniques mentioned.

Mechanism	Method	Advantage	Weakness
Saleem, Ghaffar [27]	Unique identity-based key agreement mechanism	✓ Low transmission overhead ✓ Low computation overhead	• Not support post-quantum cryptography
Lee and Chen [28]	Safe authentication mechanism for the Fog computing platform	✓ Minimizing the computational load ✓ High efficiency	• Poor performance in a real-world condition
Guo and Zhang [29]	Secured remote user authentication strategy	✓ Increasing security ✓ Reducing computation cost	• Extra complexity • High execution time
Iqbal and Bhola [30]	ECC-based secure key exchange mechanism for IoT	✓ High scalability	• Low privacy
Verma and Bhardwaj [31]	Mutual authentication and key agreement based on ECC	✓ Low overhead ✓ Reducing computing cost	• Not support key distribution • Not support key generator
Li and Miao [32]	Solution to the problems of being susceptible to internal assaults	✓ High security	• Low-power processing machine
Rana and Mishra [33]	Key agreement mechanism for the IoT ecosystem	✓ Secure in polynomial time	• High overload
Shukla and Thakur [34]	Innovative approach based on Fog computing and the blockchain	✓ Safe transactions ✓ High throughput ✓ Low packet error	• Low scalability
Wu and Lee [35]	Novel authentication key exchange system	✓ High resistance against assaults	• High memory usage
Soni and Singh [24]	Lightweight, secure health authentication, and key agreement	✓ Decreasing computing time ✓ Reducing power consumption ✓ Low execution cost	• Low reliability

Table 1. *Cont.*

Mechanism	Method	Advantage	Weakness
Hammi and Fayad [26]	OTP creation method to ensure IoT devices' security	✓ High security ✓ High throughput	• High overload • Extra complexity
Alqahtani and Al-Makhadmeh [25]	TBM strategy to enhance Cloud-assisted IoT	✓ Reducing response time ✓ Lowering detection times ✓ Increasing lifespan	• High memory consumption
Shahidinejad and Ghobaei-Arani [36]	Light-Edge authentication system	✓ Low time cost ✓ Low communication cost	• High data leaks
Abdussami and Amin [37]	Mutual authentication technique by a physically unclonable feature	✓ Low computation costs ✓ High attacks resistant	• Loss of synchronization
Erroutbi and El Hanjri [38]	Mutual authentication built on a hash-based message	✓ High scalability	• Low-power and processing machines
Proposed Mechanism	Lightweight authentication framework for mutual authentication	✓ Increasing efficiency ✓ Low communication cost	• High storage overhead

3. Proposed Mechanism

This section describes the mechanism presented to address some of the drawbacks of the prior techniques. The shorter format and notations used in this work are described in Table 2 of this document. The approach is described in greater detail in the following subsections.

Table 2. Notations and explanations.

Notation	Explanations
T	Thing
F	Fog
C	Cloud Server
IDt	Thing's Identity
TPK	Thing's Public Key
IDf	Fog Node's Identity
FPK	Fog Node's Public Key
FPR	Fog Node's Private Key
CPK	Cloud Server's Public Key
CPR	Cloud Server's Private Key
H(IPV6)	Identity of Thing's Hash
R1, R2, R3	Random Nonce

3.1. System Model

Here, it is supposed that the initial configuration of the supplied system included a trustworthy central Cloud, several Fog nodes, and several edge devices in the system. So, interaction would occur successively among the Fog node and the Cloud, the Cloud and the Fog node, and the edge-user and the Fog node. When a user wishes to access real-time information stored on a Cloud or Fog, it should also re-verify that it is a genuine user, if the edge-user wishes to determine whether the recipient of the information is an authorized node. Therefore, safe mutual authentication is of the utmost importance, as no one in the system can be trusted, and all interaction occurs across an unsafe channel.

The information might be altered if an attacker gains access to the data or the information itself. Depending on the circumstance, the verifier would create a random secret number that would be used to create the private key, only when the verification process has been completed successfully. Therefore, users and verifiers must mutually authenticate to avoid such instances. Since no session keys are produced, key management is unnecessary.

3.2. Authentication Protocol

Figure 2 depicts the planned structure, which includes representing the authentication process. Suppose that N Cloud Servers, N Fog servers, and N smart devices are placed in the system in the context of the specified framework, and, thus, smart devices are grouped in a network to form a cluster.

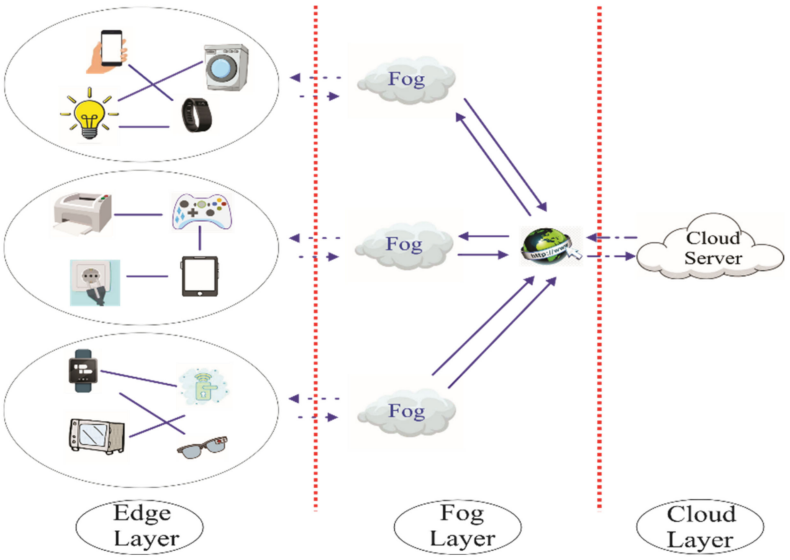

Figure 2. Specified system architecture.

As can be seen very plainly in Figure 2, many different kinds of objects, such as smart watches, home appliances, health wristbands, game consoles, computer peripherals, and so on, are clustered together and linked to the Cloud structure via the Fog layer and the Internet platform. A concise explanation of each layer's function in the Fog computing infrastructure is provided in Table 3.

Table 3. Fog computing infrastructure layers.

Notation	Explanations
Cloud Layer	This is the highest level in the Fog computing stack. Computing, networking, and storage are all handled at the Cloud layer, which is accessible from anywhere in the world. The server and data centers that make up this layer conduct a worldwide evaluation of the information they collect from the Fog layer.
Fog Layer	This is the middle and core layer and includes the switches, gateways, and routers that can also function as Fog nodesand. Any computer or machine connected to a network, which could perform localized tasks such as computing, networking, and storage, could be considered a Fog machine. The Fog node seems to be a specialized network node that can be placed anywhere along the platform's edge. It is familiar with the gadgets in its immediate vicinity and is liable for routinely uploading data to a Cloud server. The services provided by this layer to the device layer can be accessed with or without the Cloud layer being involved.
Device Layer	This is the base layer, and it includes both stationary and mobile Internet of Things gadgets. The gadgets' low processing power and memory prevent them from adapting to changing circumstances.

Two primary kinds of connection are available in the suggested model:

(1) Link from the Cloud to the Fog and vice versa;
(2) Transmission from the Fog to the gadget and vice versa.

While the conceptual approach applies to various IoT application areas, including intelligent transport systems and smart medical centers, it is not a global method, as with decentralized approaches. As a result, the suggested approach is referred to as a centralized authentication mechanism for IoT environments supported by Fog computing. The suggested plan is required for device authentication through the use of a lightweight cryptographic primitive's hashing algorithm and a randomized sequence number created by a random number generator.

The Fog server would obtain the security credentials for all smart devices. For their part, Fog servers would be provided authentication certificates by the Cloud server. When an IoT device transfers through one cluster to the other, the Fog node is in charge of authenticating the object throughout this architecture [39]. The specific Fog server where the gadget was already listed has access to the device's originating identifier and motion. The suggested paradigm, on either hand, assumes that every cluster is a network area in its own right. In the event that a thing travels between one cluster to some other, the Fog server checks the item using information out from a Cloud server and, afterward, determines if the IoT device can join the new cluster yet or not.

The suggested paradigm considers the two components of the system, including the Cloud server and the Fog server, to be resource-rich, and one system component is the IoT devices, which are incredibly resource-limited. The systems are expected to be in the form of a tree-cluster structure, with the Fog node serving as the gadget that controls the IoT items inside a certain cluster. The verification among a resource-constrained item such as an IoT device and a resource-rich item such as a Fog server is the primary issue of the present scheme. Again, another of the well-known IoT protocols, 6LoWPAN, is used to determine the identification of an IoT system. In a centralized model, a machine and a Fog server could identify each other and create a safe communication link for interaction. The recommended structure could be of great assistance in various global IoT applications, such as intelligent healthcare-based networked IoT systems, mobile-oriented dispersed IoT systems, and industrial-automation-based dispersed IoT systems.

3.3. Safety Objectives

The following are the main safety needs that are critical to providing safety for a Fog-enabled IoT domain.

- Confidentiality: This is about to be implemented to control device access.
- Integrity: The original data have not been changed.
- Accessibility: The service ought to be accessible to lawful users.
- Non-repudiation: This guarantees somebody will not be able to refute things.
- Authentication: The process of providing proof of one's identity.
- Authorization: This grant somebody permission to perform something.
- Access Control: This is who can access or utilize assets in a computing surrounding is controlled.
- Data Storage: This is constantly generating data and endpoints, sending them to the Fog nodes; since the volume of information gathered at the end of a Fog node is enormous, it is crucial to safeguard user data.
- Users Privacy: Restoration of privacy would be facilitated by limiting the study of service usage patterns and enabling authorized users only to access the assets they have.
- Location Privacy: Typically, the terminal device offloads/communicates with a neighboring Fog node. If such a Fog node is infiltrated, the hacker can determine the position of every edge device that has interacted with that node. Therefore, it is essential to protect the user's location.

- Freshness: This component guarantees that the attacker is not transmitting any earlier messages. It is, thus, guaranteeing that the information is current.
- Forward Secrecy: Just after a session has ended or the user has left or relocated, no additional communications from that user are accepted or considered.
- Backward Secrecy: When a new member joins the group, previously transmitted messages must be hidden from view.

In order to meet the criteria of the security mentioned earlier, a machine authentication mechanism for Fog-enabled IoT services must be implemented to avoid different types of attacks. When designing an authentication method for Fog computing systems, it is essential to consider how the various attacks will be shielded:

(1) A replay attack: A lawful data transfer is intentionally or illegally repeated or postponed after it has already occurred.
(2) MITM attack: In some cases, the attacker discreetly transmits and modifies the interactions among two parties.
(3) Eavesdropping: Hackers attempt to obtain personal details.
(4) Side-channel: Hacker extracts secrets from a network by analyzing physical parameters.
(5) Brute force: Assuming every possible pair of the desired password until the password is hacked.

4. Procedure of Suggested Authentication Plan

The flowchart map for the suggested authentication technique is depicted in Figure 3. When establishing a reliable connection in a system, it is necessary to implement an efficient or effective authentication system between the many connecting components (device, Fog node, and Cloud server). The five-stage identification strategy that is presented includes a preliminary stage, Fog–Cloud identification, a stage for device registering, a stage for Fog–Thing mutual authentication, and a stage for verification in intercluster motion that will presume that the ID of the Fog node has already been stored into the Cloud server. Since the Fog node is a component of the Cloud server, this is a straightforward process.

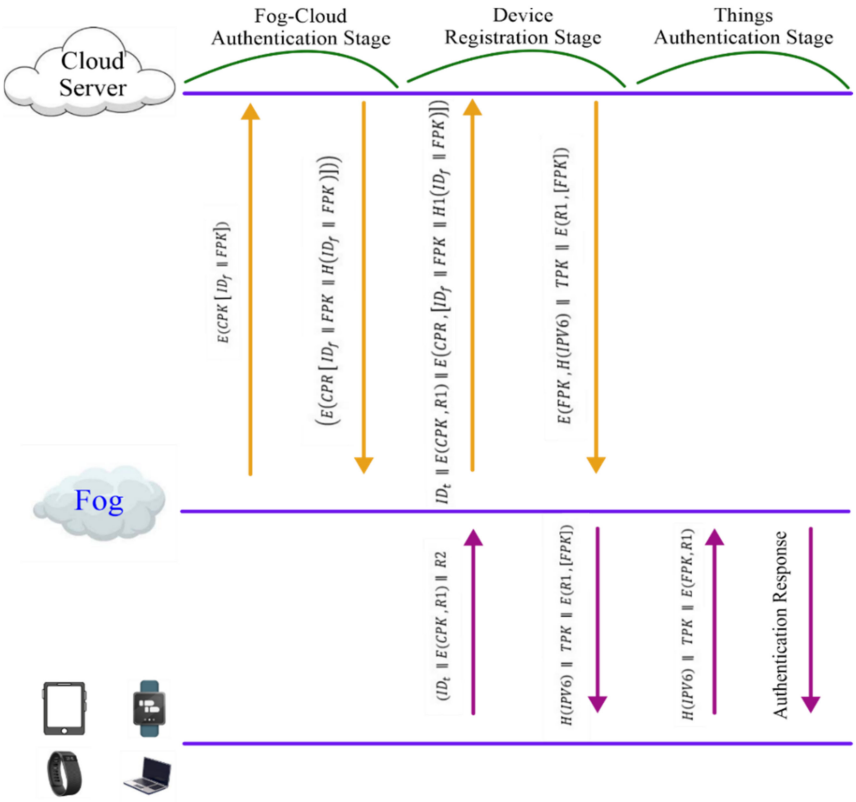

Figure 3. Flowchart of the planned authentication mechanism.

Stage 1: Preliminary

The TTP is responsible for obtaining Cloud, Fog, and device registrations prior to their installation in a dispersed system during this stage. The suggested approach relies on an asymmetric encryption technique for key generation, with the hashing method being employed to generate the hash value. The Cloud server uses asymmetric encryption to establish a public/private pair of keys for the devices, and the Fog server uses asymmetric encryption to create its own key pair for the gadget. As previously stated, it will be supposed that the Cloud's public key is cached into every IoT device at the production stage.

Stage 2: Identification between the Cloud Server and Fog Node

During this stage, the Fog node and Cloud server identify with one another on a cooperative basis. The Fog node delivers its ID_f alongside their public key, which is secured with the public key of Cloud $E\left(CPK\left[\ ID_f\ \|\ FPK\right]\right)$. Cloud E receives its ID_f alongside its public key. Upon receiving a message, the Cloud server decodes using the Cloud's private key and obtains the ID of the Fog node as well as the public key of the Fog node. The Cloud server would validate the Fog node's identification by matching the Fog node's decoded ID with the Fog node's public key. When confirming the identification of the Fog node, the Cloud replies with a text that has been encoded with the Cloud's private key $\left(E\left(CPR\left[\ ID_f\ \|\ FPK\ \|\ H\left(ID_f\ \|\ FPK\right)\right]\right)\right)$.

This communication is referred to as a certificate, and it is produced by the Cloud server. The hash identification of the Fog node is represented by $H\left[\ ID_f\ \|\ FPK\right]$. The Fog node decodes the certificate, after receiving it from the Cloud server, using the Cloud's public key, and verifies the identification of the Cloud server, since only genuine Clouds are able to obtain the ID and public key of the Fog node; when receiving the certificate from the Cloud server, both the Cloud and the Fog are fully verified with one another during this stage.

Stage 3: Registration of Devices

This stage serves as a requirement for the real verification process, which follows after it. According to the suggested system, an IoT item makes an authentication request to a Fog node, which contains its unique identifier ID_t and a completely random sequence number (*R1*). IP, MAC, Zigbee address, and other types of networks would determine the identity of the item, and nonce R1 would serve as a private key encoded by the Cloud's public key $E(CPK,\ R1)$. It is, therefore, necessary to send a second nonce (*R2*) in order to avoid a replay attack $[ID_t\ \|\ E(CPK,\ R1)\ \|\ R2]$. Later, the Fog node receives an authentication process from the device and does an initial identity validation on the IoT device.

The term "preliminary identity check" refers to the process of checking/verifying the address of the source of a Fog node. The source address in the register query is checked by the Fog node during this confirmation, since the Fog node is knowledgeable of the communication protocol that is employed in a limited network environment. To identify itself, the Fog node makes a request to the Cloud along with a copy of its certificate, which is then verified by a Cloud server $ID_t\ \|\ E(CPK,\ R1)\ \|\ E\left(CPR,\ \left[ID_f\ \|\ FPK\ \|\ H1\left(ID_f\ \|\ FPK\right)\right]\right)$. Employing asymmetric encryption, the Cloud generates an *IPV6* address and public key for the gadget, with an incoming nonce (*R1*) serving as the device's private key within this scenario.

Information produced by a Cloud server includes the following information:

✓ *IPV6* hash identification;
✓ Objects that have a public key *TPK*;
✓ The thing's private key encrypted by the Fog's public key.

These data have been encoded using the public key of the Fog's encryption algorithm. $E(FPK,\ H(IPV6)\ \|\ TPK\ \|\ E(R1,\ [FPK])$ is received by the Fog node, which performs

decoding on it. The Fog node would save the hashed identifier $H(IPV6)$ and the associated items public key upon completing the decoding process. Toward the end of this stage, the Fog node delivers a message to the object that has the following details: the object's public key and hash address and the Fog node's public key secured by the gadget's private key, among other items. The gadget checks that this is being connected to the Cloud server when getting a message $H(IPV6) \parallel TPK \parallel E(R1, [FPK])$. The equipment does this by getting the public key of the Fog node encoded with its private key. Within this situation, the machine decodes and saves the public key of the Fog node on its internal storage.

Stage 4: Mutual Identification between the Fog and Device

To identify itself, the object transmits a cached $H(IPV6)$ together with a nonce ($R3$), which is confirmed by the Fog's public key, in place to avert replay attacks and to validate the Fog node: $H(IPV6) \parallel TPK \parallel E(FPK, R3)$. A Fog node will conduct decoding and search for its public key inside its internal storage as soon as it receives this information from the central server. The Fog node compares the incoming hashed identification of the object with the item's pre-stored hashed identity. A Fog node has properly validated a device when both of its IDs exactly match. Lastly, the Fog node communicates with the object by sending an authentication reply.

Stage 5: Authentication during the Inter-cluster Movement

The migration of a gadget through one cluster to others is taken into consideration in this stage of the process. That is the responsibility of the existing or visiting Fog node, with the assistance of the Cloud server, to identify the devices in that circumstance. A device moving to some other cluster would cause the present Fog node not to be able to locate the hashed identification of object $H(IPV6)$ inside its database. The Fog node would then inquire of the Cloud server whether or not the visiting item is authorized, which has a worldwide database that stores the hashed identity of each registered device on the Cloud server.

After finding the $H(IPV6)$ of the currently viewed item, the Cloud sends the $H(IPV6)$ of that object to the Fog node, including the device's public key, if it has been located. When this is completed, the Fog node decodes the nonce, saves it, and uses it to identify the thing. If there is failure to authenticate the equipment by a Fog node, the currently accessed machine in a given cluster is deemed to be an alien by the Fog network. The authentication procedure offered here is exclusively for registered devices, not really for machines from out of the network or from the Internet. Before the verification procedure can begin, all external devices should be registered.

Precisely, three vital positions are specified in the planned authentication process: IoT devices, the Fog node, and the Cloud server. In all of the position sections, the relevant information, a basic step, and a number of changes are defined.

4.1. Security Evaluation

The safe architecture for three-way authentication service is provided in order to avoid unwanted access to IoT gadgets within the cluster as well as the inter-cluster transfer of items across clusters of devices. Section 3.2 discusses a series of generic grouped attacks, but this section examines the safety properties of the suggested approach within the setting of that set.

I. Protect against Brute Force

The hacker attempts to guess the private key throughout this attack using every possible combination. Asymmetric encryption techniques and a one-way hashing are employed in the designed system, which provides strong resistance versus brute force attacks.

II. Protect against Side-Channel

In this scenario, the hacker calculates the secret exponent by leveraging the time variance of the encryption procedure when computing the duration. This is because a one-

way hashing and an asymmetric technique have been utilized in the registration process to safeguard the data from this type of hacking assault.

III. Protect against MITM

It is necessary to use an encrypted nonce (*R1*) and mutual authentication among the gadget and the Fog, in order to prevent the proposed approach against MITM attacks. In order to accomplish the above, the gadget creates and calculates $(ID_t \parallel E(CPK, R1) \parallel R2$ and outputs the result to the Fog node, which then transmits the message to the Cloud for validation. The entire process serves to prevent a MITM assault.

IV. Protect against Eavesdropping

This attack was carried out in order to obtain access to confidential information that was not allowed. Encryption techniques can be used to prevent eavesdropping in conversations. Communication between the elements such as the Fog, Cloud, and items is encrypted in the proposed framework, in order to prevent eavesdropping on the conversation. According to the cryptographic theory model, an attacker would be unable to decrypt data without a key. In this concept, an asymmetric method is utilized for encryption, and a powerful one-way hash function is employed in conjunction with it.

V. Protect against Node Capture

The authentication method involves IoT devices selecting a randomized nonce that would be deleted whenever the connection comes to an end.

VI. Protect against Replay Attacks

It is possible to collect data among objects and replay them falsely in this assault, if the attacker has access to information across things. The use of a private nonce could prevent this assault from occurring. In place to avert replay attacks, a unique nonce is generated for each session. The hacker has a nonce in order to obtain data, but, according to past research, it is challenging to generate a different nonce each time.

4.2. Appraisal of the Designed System

Scalability, efficiency, and security are all demonstrated in the following sub-sections.

(1) Increased Scalability and Response Time

Various dispersed IoT apps could benefit from the suggested architecture, including intelligent healthcare systems, intelligent transport systems, and other apps in which connection latency is critical. As a result, such a form of application requires a faster reaction time in order to meet client needs. Compared to earlier research, the suggested scheme makes use of a number of strategies that make the Fog-enabled IoT architecture increasingly scalable. The use of Fog-based identification has reduced the reliance on the Cloud server's verification. As a result, the verification system would be quicker and more scalable. Moreover, the use of a three-way authentication technique in conjunction with a Cloud server would improve the capacity to manage authentication for an impressive number of IoT objects.

(2) Effectiveness

Through the establishment of reasonable and logical connections among Fog devices and Cloud–Fog servers throughout the process of verification, the suggested scheme has made the authentication system more efficient for all parties involved. As a result, with the assistance of the Cloud server, the Fog node and IoT devices are mutually verified, and the Cloud server would certify the identification of the IoT devices. Throughout such an addition, the position of the Fog node, in the interest of maintaining and obtaining IoT devices with the help of encryption algorithms within a cluster, is another characteristic of the suggested scheme that significantly increases the efficiency of the IoT ecosystem by greatly depending on Fog technology.

(3) Safety and Protection

Moreover, with the assistance of cryptographic operations, the overall security of the proposed architecture has been enhanced. Due to the use of an asymmetric cryptographic method and a one-way hash during the verification process, confidence in the architecture would grow more quickly.

5. Performance Analysis

Here, how well the proposed authentication method works when resources are limited is evaluated. Device identifiers, nonces, and random numbers are all assumed to be 128 bits in length. The hash function's output is treated as 256 bits. However, only the costs associated with device communication and storage are considered.

5.1. Communication Cost

The cost of sending messages between interacting entities is referred to as the communication cost. It is the cost associated with transmitting security parameters from the things to the Fog. Figure 4 presents a comparison of the various protocols' costs associated with the communication. Regarding the cost of communication, the suggested protocol is more advantageous than the one already used [40–43].

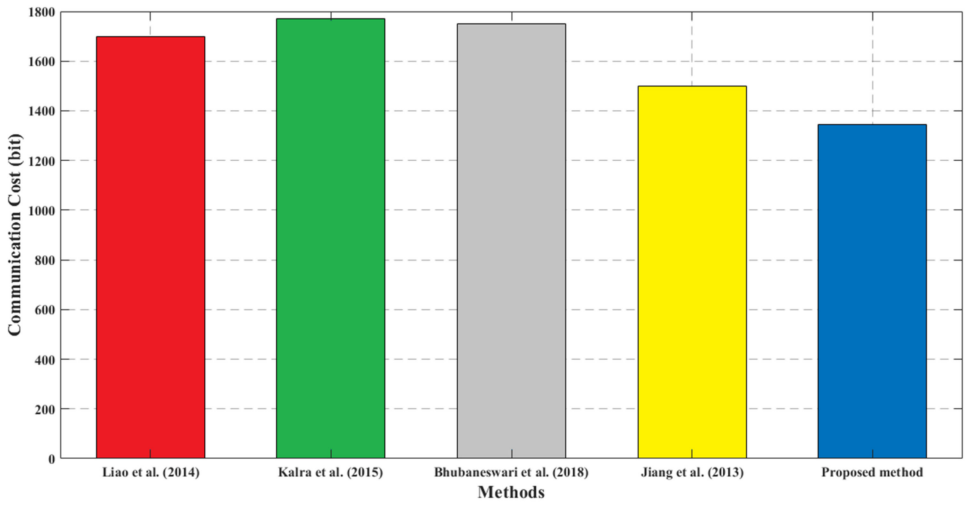

Figure 4. Communication cost.

5.2. Storage Overhead

Figure 5 depicts the IoT device's storage overhead, which is higher than the related protocols. The explanation for this is that the proposed scheme guarantees device anonymity, whereas other protocols [40,42] do not. The suggested protocol provides mutual authentication using a 256-bit hash cryptosystem, whereas other protocols [41–43] are unable to provide mutual authentication.

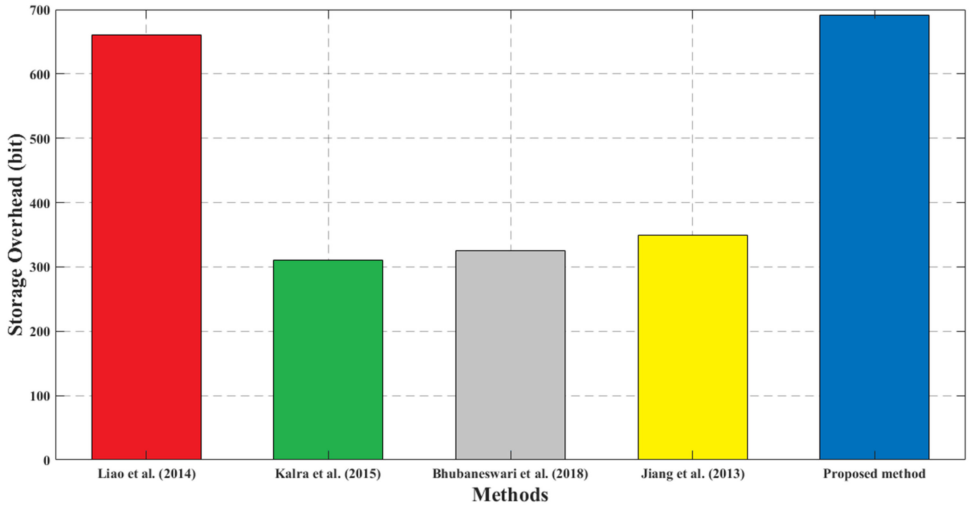

Figure 5. Storage overhead.

6. Conclusions and Future Works

The IoT is the most viable idea available these days. In resource-constrained surroundings, heavyweight verification options are not workable for verification. As a result, environmental resource constraints are taken into account when developing a solid authentication system. Utilizing cryptographic techniques and asymmetric cryptographic operations, a lightweight authentication mechanism is being developed for IoT devices connected to the Fog network. For the authentication between the gadget and the Fog, lightweight encryption algorithms are employed, and asymmetric procedures are implemented for the identification between the Fog and the Cloud server. In accordance with security analysis, the proposed authentication system fulfills the requirements for mutual authentication as well as secrecy.

The future effort will improve the proposed method with the least amount of computational overhead possible. For future work, there is a need for more modifications to be made to use this method in various contexts such as BLE or Zigbee, which are consistently being developed. In order to make this protocol better suitable for mutual authentication across low-power and processor devices, the focus is on upgrading it by tweaking several variables of the Hash-based Message Authentication Code (HMAC) mechanism, which will also improve the proposed method with the least possible amount of overhead.

Author Contributions: Conceptualization, J.L., M.S., A.M.R., M.H.M., F.K. and M.H.; data curation, J.L., M.S., A.M.R. and M.H.; formal analysis, A.M.R., M.H.M. and F.K.; investigation, J.L., M.S., F.K. and M.H.; methodology, J.L., M.H.M. and M.H.; project administration, J.L., M.S. and F.K.; supervision, J.L., F.K. and M.H.; validation, J.L. and M.S.; visualization and writing—original draft, M.H.M. and M.H.; writing—review and editing, M.S., A.M.R. and F.K. All authors have read and agreed to the published version of the manuscript.

Funding: The result was created by solving the student project "Security analysis and developing lightweight ciphers and protocols", using objective-oriented support for specific university research from the University of Finance and Administration, Prague, Czech Republic.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors thank Michal Merta and Zdeněk Truhlář for their help with the research connected with this article.

Conflicts of Interest: The authors declare that this manuscript is original, has not been published before, and is not currently being considered for publication elsewhere. There are no conflicts of interest in this research.

References

1. Sadrishojaei, M.; Navimipour, N.J.; Reshadi, M.; Hosseinzadeh, M.; Unal, M. An energy-aware clustering method in the IoT using a swarm-based algorithm. *Wirel. Netw.* **2022**, *28*, 125–136. [CrossRef]
2. Pokhrel, S.R.; Verma, S.; Garg, S.; Sharma, A.K.; Choi, J. An efficient clustering framework for massive sensor networking in industrial Internet of Things. *IEEE Trans. Ind. Inform.* **2020**, *17*, 4917–4924. [CrossRef]
3. Sadrishojaei, M.; Navimipour, N.J.; Reshadi, M.; Hosseinzadeh, M. A new clustering-based routing method in the mobile internet of things using a krill herd algorithm. *Clust. Comput.* **2021**, *25*, 351–361. [CrossRef]
4. Yousefi, S.; Derakhshan, F.; Aghdasi, H.S.; Karimipour, H. An energy-efficient artificial bee colony-based clustering in the internet of things. *Comput. Electr. Eng.* **2020**, *86*, 106733. [CrossRef]
5. Rahmani, A.M.; Naqvi, R.A.; Malik, M.H.; Malik, T.S.; Sadrishojaei, M.; Hosseinzadeh, M.; Al-Musawi, A. E-Learning Development Based on Internet of Things and Blockchain Technology during COVID-19 Pandemic. *Mathematics* **2021**, *9*, 3151. [CrossRef]
6. Sadrishojaei, M.; Navimipour, N.J.; Reshadi, M.; Hosseinzadeh, M. An Energy-Aware IoT Routing Approach Based on a Swarm Optimization Algorithm and a Clustering Technique. *Wirel. Pers. Commun.* **2022**, 1–17. [CrossRef]
7. Khanna, A.; Kaur, S. Internet of things (IoT), applications and challenges: A comprehensive review. *Wirel. Pers. Commun.* **2020**, *114*, 1687–1762. [CrossRef]
8. Ahmad, W.; Ahmad, W.; Rasool, A.; Javed, A.R.; Baker, T.; Jalil, Z. Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey. *Electronics* **2021**, *11*, 16. [CrossRef]
9. Yu, Z.; Song, L.; Jiang, L.; Sharafi, O.K. Systematic literature review on the security challenges of blockchain in IoT-based smart cities. *Kybernetes* **2021**, *51*, 323–347. [CrossRef]
10. Wu, Y. Cloud-edge orchestration for the Internet of Things: Architecture and AI-powered data processing. *IEEE Internet Things J.* **2020**, *8*, 12792–12805. [CrossRef]
11. Sadrishojaei, M.; Navimipour, N.J.; Reshadi, M.; Hosseinzadeh, M. A new preventive routing method based on clustering and location prediction in the mobile internet of things. *IEEE Internet Things J.* **2021**, *8*, 10652–10664. [CrossRef]
12. Hashmi, S.A.; Ali, C.F.; Zafar, S. Internet of things and cloud computing-based energy management system for demand side management in smart grid. *Int. J. Energy Res.* **2021**, *45*, 1007–1022. [CrossRef]
13. Barik, R.K.; Patra, S.S.; Patro, R.; Mohanty, S.N.; Hamad, A. GeoBD2: Geospatial big data deduplication scheme in fog assisted cloud computing environment. In Proceedings of the IEEE 8th International Conference on Computing for Sustainable Global Development, New Delhi, India, 17–19 March 2021.
14. Sarrab, M.; Alshohoumi, F. Assisted-fog-based framework for IoT-based healthcare data preservation. *Int. J. Cloud Appl. Comput.* **2021**, *11*, 1–16. [CrossRef]
15. Fu, C.; Lv, Q.; Badrnejad, R.G. Fog computing in health management processing systems. *Kybernetes* **2020**, *49*, 2893–2917. [CrossRef]
16. Stergiou, C.L.; Psannis, K.E.; Gupta, B.B. IoT-based big data secure management in the fog over a 6G wireless network. *IEEE Internet Things J.* **2020**, *8*, 5164–5171. [CrossRef]
17. Firouzi, F.; Farahani, B.; Marinšek, A. The convergence and interplay of edge, fog, and cloud in the AI-driven Internet of Things (IoT). *Inf. Syst.* **2022**, *107*, 101840. [CrossRef]
18. Firouzi, F.; Chakrabarty, K.; Nassif, S. *Intelligent Internet of Things: From Device to Fog and Cloud*; Springer: Berlin/Heidelberg, Germany, 2020.
19. Yang, X.; Rahmani, N. Task scheduling mechanisms in fog computing: Review, trends, and perspectives. *Kybernetes* **2020**, *50*, 22–38. [CrossRef]
20. Al-Qerem, A.; Alauthman, M.; Almomani, A.; Gupta, B.B. IoT transaction processing through cooperative concurrency control on fog–cloud computing environment. *Soft. Comput.* **2020**, *24*, 5695–5711. [CrossRef]
21. Sadrishojaei, M.; Navimipour, N.J.; Reshadi, M.; Hosseinzadeh, M. Clustered Routing Method in the Internet of Things Using a Moth-Flame Optimization Algorithm. *Int. J. Commun. Syst.* **2021**, *34*, e4964. [CrossRef]
22. Mabodi, K.; Yusefi, M.; Zandiyan, S.; Irankhah, L.; Fotohi, R. Multi-level trust-based intelligence schema for securing of internet of things (IoT) against security threats using cryptographic authentication. *J. Supercomput.* **2020**, *76*, 7081–7106.
23. Kalyani, G.; Chaudhari, S. An efficient approach for enhancing security in Internet of Things using the optimum authentication key. *Int. J. Comput. Appl.* **2020**, *42*, 306–314. [CrossRef]
24. Soni, M.; Singh, D.K. LAKA: Lightweight authentication and key agreement protocol for internet of things based wireless body area network. *Wirel. Pers. Commun.* **2021**, 1–18. [CrossRef]
25. Alqahtani, F.; Al-Makhadmeh, Z.; Tolba, A.; Said, O. TBM: A trust-based monitoring security scheme to improve the service authentication in the Internet of Things communications. *Comput. Commun.* **2020**, *150*, 216–225. [CrossRef]
26. Hammi, B.; Fayad, A.; Khatoun, R.; Zeadally, S.; Begriche, Y. A lightweight ECC-based authentication scheme for Internet of Things (IoT). *IEEE Syst. J.* **2020**, *14*, 3440–3450. [CrossRef]

27. Saleem, M.A.; Ghaffar, Z.; Mahmood, K.; Das, A.K.; Rodrigues, J.J.P.C.; Khan, M.K. Provably Secure Authentication Protocol for Mobile Clients in IoT Environment using Puncturable Pseudorandom Function. *IEEE Internet Things J.* **2021**, *8*, 16613–16622. [CrossRef]
28. Lee, T.-F.; Chen, W.-Y. Lightweight fog computing-based authentication protocols using physically unclonable functions for internet of medical things. *J. Inf. Secur. Appl.* **2021**, *59*, 102817. [CrossRef]
29. Guo, Y.; Zhang, Z.; Guo, Y. SecFHome: Secure remote authentication in fog-enabled smart home environment. *Comput. Netw.* **2022**, *207*, 108818. [CrossRef]
30. Iqbal, U.; Bhola, J.; Jayasudha, M.; Ahmad, M.W.; Neware, R.; Yadav, A.R.; Gelana, F.W. ECC-Based Authenticated Key Exchange Protocol for Fog-Based IoT Networks. *Secur. Commun. Netw.* **2022**, *2022*, 7264803. [CrossRef]
31. Verma, U.; Bhardwaj, D. A secure lightweight anonymous elliptic curve cryptography-based authentication and key agreement scheme for fog assisted-Internet of Things enabled networks. *Concurr. Comput Pract. Exp.* **2022**, *34*, e7172. [CrossRef]
32. Li, Z.; Miao, Q.; Chaudhry, S.A.; Chen, C.-M. A provably secure and lightweight mutual authentication protocol in fog-enabled social Internet of vehicles. *Int. J. Distrib. Sens. Netw.* **2022**, *18*, 15501329221104332. [CrossRef]
33. Rana, S.; Mishra, D.; Arora, R. Privacy-Preserving Key Agreement Protocol for Fog Computing Supported Internet of Things Environment. *Wirel. Pers. Commun.* **2021**, *119*, 727–747. [CrossRef]
34. Shukla, S.; Thakur, S.; Hussain, S.; Breslin, J.G.; Jameel, S.M. Identification and Authentication in Healthcare Internet-of-Things Using Integrated Fog Computing Based Blockchain Model. *Internet Things* **2021**, *15*, 100422. [CrossRef]
35. Wu, T.-Y.; Lee, Z.; Yang, L.; Luo, J.-N.; Tso, R. Provably secure authentication key exchange scheme using fog nodes in vehicular ad hoc networks. *J. Supercomput.* **2021**, *77*, 6992–7020. [CrossRef]
36. Shahidinejad, A.; Ghobaei-Arani, M.; Souri, A.; Shojafar, M.; Kumari, S. Light-edge: A lightweight authentication protocol for IoT devices in an edge-cloud environment. *IEEE Consum. Electron. Mag.* **2021**, *11*, 57–63. [CrossRef]
37. Abdussami, M.; Amin, R.; Vollala, S. LASSI: A lightweight authenticated key agreement protocol for fog-enabled IoT deployment. *Int. J. Inf. Secur.* **2022**, *21*, 1373–1387. [CrossRef]
38. Erroutbi, A.; El Hanjri, A.; Sekkaki, A. Secure and Lightweight HMAC Mutual Authentication Protocol for Communication between IoT Devices and Fog Nodes. In Proceedings of the IEEE International Smart Cities Conference (ISC2), Casablanca, Morocco, 14–17 October 2019.
39. Singh, S.; Bansal, A.; Sandhu, R.; Sidhu, J. Fog computing and IoT based healthcare support service for dengue fever. *Int. J. Pervasive Comput. Commun.* **2018**, *14*, 197–207. [CrossRef]
40. Jiang, R.; Lai, C.; Luo, J.; Wang, X.; Wang, H. EAP-based group authentication and key agreement protocol for machine-type communications. *Int. J. Distrib. Sens. Netw.* **2013**, *9*, 304601. [CrossRef]
41. Liao, Y.-P.; Hsiao, C.-M. A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol. *Ad Hoc Netw.* **2014**, *18*, 133–146. [CrossRef]
42. Kalra, S.; Sood, S.K. Secure authentication scheme for IoT and cloud servers. *Pervasive Mob. Comput.* **2015**, *24*, 210–223. [CrossRef]
43. Bhubaneswari, S.; Ananth, N. Enhanced mutual authentication scheme for cloud of things. *Int. J. Pure Appl. Math.* **2018**, *119*, 1571–1583.