Proposed Authentication Protocol for IoT using Blockchain and Fog Nodes

Ahmed Nabil Abdalah[1]
Faculty of Graduate Studies
for Statistical Research
Cairo University

Ammar Mohamed[2]
Faculty of Computer Science
Misr International university
On leave Faculty of graduate studies
Cairo university

Hesham A. Hefny[3]
Faculty of Graduate Studies
for Statistical Research
Cairo University

***Abstract*—The IoT offers enormous opportunities and also brings some challenges. Authentication considered one of the main challenges introduced by IoT. IoT devices are not able to protect themselves due to there limited processing and storage capabilities. Researchers proposed authentication algorithms with either a lack of scalability or vulnerable to cyberattacks. In this paper, we propose a decentralized token-based authentication based on fog computing and blockchain. The protocol provides a secure authentication protocol using access token, ECC cryptography, and also blockchain as decentralized identity storage. The blockchain uses cryptographic identifiers, records immutability, and provenance, which allows the implementation of a decentralized authentication protocol. These features ensure a light and secure identity management system. We evaluate this protocol communication between controller, gateways, and devices using AVISPA/ HLPSL, and results obtained from AVISPA simulation shows that our protocol is safe based on secrecy and strong authentication criteria. The paper uses four test cases to test the Ethereum smart contract implementation to ensure the system functions properly.**

***Keywords*—Internet of Things; smart contract; blockchain; fog computing; authentication; access token**

I. Introduction

The rapid growth in the connected devices and networks formed what we called the Internet of Things (IoT). Nowadays, IoT devices are capable of communicating, collaborating, and also can be remotely managed. All these capabilities led to using IoT in many several domains, e.g., public health, intelligent grids, smart business, waste management, smart houses, smart cities, farming, energy management [1]. In 1995 only 0.4% of the total world population was using the internet. This number increased in 2019 to be 57% of the world population [2]. This means the network expanded and became more open. On the other hand, security and privacy did not evolve enough to handle this huge increase in the number of connected devices, which has an impact on data protection and privacy over the network.

One significant difference between IoT and the traditional networks is human interaction. The nature of the IoT devices is to observe personal data, analyze and perform actions based on their analysis, which makes IoT devices obtain a large amount of data, and some of the data is private. For this reason, digital identity is vital for IoT networks as this data can be exposed or misused [3] [4]. while looking into the data protection concerns, we should consider that most of the IoT devices are limited in terms of the processing and storage capacities [5].

The growth in the IoT connected devices without having a robust authentication protocol allows the intruder to gain access to a wide range of data and private information on a large scale. Besides, most of the users are unaware of the security concerns and issues of there IoT devices. For example, Xiongmai Technology recalled 4.3 million cameras for a security bug that made them vulnerable against cyberattacks [6].

They said that "The elements of security in computing begin with Identity" [7]. Digital identity and authentication, act as an essential foundation for IoT networks as they make communication, data exchange, and transactions possible. When structuring a digital identity framework, various concerns must be taken into account, for instance, practicability, user-friendliness, data protection, prevention of misuse, and the guaranteeing of autonomy in terms of information [8]. There are many problems with traditional identity management systems, as proven by the many cyberattacks that leaked personal information [9], [10]. These systems are not suitable for IoT, besides most of these systems use centralized identity storage, which considered as a single point of failure [11]. For these reasons, IoT identity systems should use decentralized storage. One of the common decentralize storage is Blockchain as it provides secure, private, efficient storage.

IoT can take advantage of fog computing to deploy a set of nodes that can support authentication. These nodes are synced and managed by a central authority controller. These nodes are capable of storing identities in Blockchain, which ease the authentication of users and devices.

The main goal of this paper is to propose an authentication protocol that provides device authentication based on blockchain and fog nodes. The proposed protocol uses elliptic curve cryptography(ECC) based certificates, which are smaller and faster to generate. This advantage makes it a perfect choice for IoT networks as it solves the limitation of IoT processing and storage resources [5]. The massive number of transactions will affect any centralized storage and make it a single point of failure, therefore we use Ethereum Blockchain as decentralizing and distributed identity storage. Another advantage of the Ethereum Blockchain is the smart contract feature, which enables the implementation of custom logic inside the Blockchain. The Fog computing choice helps to recognize and block cyberattacks. They are closer to IoT devices, which

reduce latency and allow them to move heavy processing tasks to the Fog nodes [12]. This advantage decreased the processing burden of the IoT devices. The proposed system allows the IoT devices to operate autonomously and securely after an initial configuration done by the user.

The rest of this paper organized as follows: in Section II, survey related work. In Section III, present the background of the topics, which gives brief notes on each topic discussed in this paper. In Section IV, present the proposed architecture in detail. In Section V, present the evaluation and results. Finally, present the conclusion in Section VI.

II. Related Work

Improving IoT identity and authentication has been an active research field for years, many identity/ authentication already proposed, there are some of these different studies.

In [13], Chen Ju and Liu Y proposed an identity Management Framework for the Internet of Things. They focus on three critical issues of Identity management for IoT and present an IDM framework for IoT, which consists of the standard identity information model, user-centric architecture, and multi-channel authentication model. The user-centric IDM architecture allows the user to get access to different IoT services by different authentication methods without maintaining multiple identities.

In [14], the authors proposed an identity approach for IoT that can benefit from the software-defined network (SDN) and fog computing to deploy an authentication layer by implementing a centralized authentication layer to over the SDN controller. In this approach, they assume that every IoT device has IPv6 and supports the TCP/IP. One of the limitations of using a centralized security approach is scalability, and also centralized identity storage considers as a single point of failure [11]. In this paper proposed protocol, uses decentralized identity storage (Blockchain) to avoid these limitations.

In [15], Van, P.Butkus, and D. Van Thanh have proposed user-centric identity management for IoT that addresses a future environment where billions of people and things are interacting and collaborating in a dynamic based on the identities of the users and relationships between users. The usefulness of the solution demonstrated in the typical use case of visiting friends in which a user visits his friends and his/her devices are allowed to engage communication and collaboration with devices at the visited place, the implemented approach proposed three layers. 1. Device Subsystem (DS) is a middle-ware layer on a user's device, which provides authentication functions to applications. 2. Service Subsystem (SS) is located on the Service Provider server and provides functions to delegate authentication to IDPs and to enforce service access control 3. Identity Provider Subsystem (IDPs) is located on the Identity Provider server and responsible for the storage of all the identity data as well as the authentication of users/devices and services. It can be a private or public entity, installed by a private user at home or a public party in a cloud, respectively.

In [16], Michal and Timas proposed A centralized Identity Management for devices in the Internet of things. They store devices unique identifier and also support role-based access control, In this approach system administrator will initiate this process by creating device account on the identity store and configure the device to use this identity store, after that device should communicate with the identity store for authentication and authorization, means it will have so many requests to the identity store which could be a bottleneck when many devices communicating at the same time.

In [17], Makoto Takemiya, and Bohdan Vanieiev proposed a model to store identity using the Blockchain and based on the JSON-LD key. This model put the user in control of his identity, as the user will use a mobile app that able to communicate with Blockchain to store encrypted personal information, in this model some attributes are necessary to justify, and one major drawback is there is no way to retrieve user data if the user lost or replaced his phone.

In [18], the authors proposed an authentication scheme using blockchain-enabled fog nodes. These fog nodes communicate with Ethereum smart contracts to execute some logic that helps to authenticate users to access IoT devices. They used Fog nodes to provide scalability and carrying out heavy processing tasks related to authentication and Blockchain handling to Fog nodes, there proposed model is consist of admins, end-users, fog nodes, IoT devices, and cloud. The proposed approach suggests that Fog nodes are managing authentication and access to IoT devices, and also managing the Ethereum network throw smart contracts. Administrators are responsible for managing fog nodes and their associated IoT devices.

In [19], D. Li, W. Peng, W. Deng, and F. Gai proposed a lightweight authentication system that depends on public-key and private keys cryptography and Blockchain for Iot authentication. To prevents single-point failure and also to ensure that the system will not go down even if some nodes are under DDoS attacks. In this approach, each IoT device registered in the Blockchain. As a result of the registration step device ID, a hashed data and public key stored in the Blockchain. Each node generates there private and public keys using (CSPRNG) and these public keys stored in the Blockchain.

In [20] authors proposed a threshold cryptography-based group authentication (TCGA) scheme for the IoT. This algorithm consists of five main functions: key distribution, key update, group credit generation, authentication listener, and message decryption. (TCGA) is designed to work with Wi-Fi networks and provides authentication for a group of IoT devices in the group communication model.

III. Background

Internet of things (IoT) became very popular in the past few years, The phrase "Internet of Things" consists of two words, the first word is "Internet" and the second word is "Things". Internet is the global system of interconnected computer networks that use Internet protocols (TCP/IP) to serve services to devices worldwide. Therefore the internet is a network of networks that consists of private and public networks. Internet users raised from 413 million in 2000 to over 3.4 billion in 2016 [21]. While the definition of Thing could be an object or a person, we see new objects that can connect to the internet as Things. Things are not limited to electronic devices but also Things that we never think of

like clothing, furniture, materials, Spare Parts and equipment, merchandise and specific items, landmarks, monuments and works, culture and sophistication [22]. IoT is a network of things that allows things to connect, interact, and exchange data.

Identity management (IdM) also known as (IAM or IdAM), It is the task needed for generating, storing, and managing permission for users and computers. Saved identity allows the IdM to authenticates and authorize users to access services and resources.

It also includes and manages descriptive information about the user. IdM authorizes read and write access to this information. Establishing an identity management approach in the IoT networks can be a challenging task from a software architecture and implementation perspective because of diversity in technologies, standards, and identity management implementations.

Cryptography is a way to guard information and communication. Based on mathematical theories and algorithms to transform messages into a form that is hard to decrypt. These algorithms are used in cryptographic key generation, digital signing, and verification to protect data privacy, internet browsing, emails, and confidential financial communications such as credit card transactions. There are two encryption algorithms single-key algorithm and symmetric-key algorithm both algorithms generate a fixed-length secret key that the sender used to encrypt the message, and the receiver uses it to decrypt the message. Elliptic-curve cryptography (ECC) is a cryptography algorithm built based on the algebraic structure of elliptic curves over finite fields. ECC uses smaller keys that are smaller than RSA keys, which make ECC keys generation are significantly faster than RSA [23]. The time required to generate the RSA key, and also the key length makes ECC a better choice for IOT devices where storage and processing are relatively limited. Also, ECC is less vulnerable to Quantum Computing.

Fog computing is a distributed network that fills the gap between data and cloud computing. Fog computing empowers more processing duties to perform at the edge nodes. That would enable more opportunities that were not there before as due to the limitation of the IoT devices. Heavy processing tasks cannot be performed on these devices. At the same time, cloud computing latency will make it almost impossible to move these tasks to cloud computing. Using Fog nodes will give the IoT devices the ability to react more quickly to events, and also, Fog computing prevents cloud computing issues like network congestion, delay, and privacy concerns [24] if the data processing is happening on the cloud.

Blockchain is a linked list of blocks. Each block contains a transaction, a timestamp, and a hash of the previous block for linking. Blockchain technology is developed based on the vision of creating a decentralized, distributed, and encrypted system that can take over the traditional central organizational storage system and is to make transactions possible directly between the given network's participants. The most famous application by no means, the only one is the cryptocurrency such as Bitcoin [25]. The growth in bitcoin transactions led to a massive upsurge in energy consumption due to Cryptocurrency mining [26]. Just recently, applications beyond the cryptocurrency context are increasingly moving into focus. Blockchain is not only used for money transactions but also used in other domains. For example, the Ethereum platform can execute Turing-complete programs called Smart Contracts. Ethereum smart contract is a decentralized application that exists in the Ethereum Blockchain gives blockchain the ability to execute custom logic on transactions. However, smart contracts can not fetch external data and execute functions on its own. Despite smart contracts providing computation ability, every transaction should be able to verify.

To evaluate authentication protocol, this can be done using model checking tools. In this research, the evaluation of the proposed protocol performed by using the protocol analysis tool, AVISPA, which stands for Automatic Validation of Internet Security Protocols and Applications [27]. In order to validate a protocol, A formal language HLPSL (High-Level Protocols Specification Language) used by AVISPA. HLSPL is a role-based language as any protocol consists of multiple roles each role contains a set of transitions that specify pre and post conditions of the role also a goal should be set for each protocol. There are two goals types of secrecy, which make sure that the intruder should not decrypt the value set in secrecy. The second goal is weak authentication this goal make sure that roles should have a strong authentication means each role should authenticate the received request.

IV. Proposed Architecture

In this section, we propose an enhanced authentication protocol. We assume that every IoT device, controller, and the gateway has a pre-embedded identifier. Also, the cloud server has a list of controllers addresses, and the cloud server account will register the list of controllers right after deploying the smart contract. The proposed architecture contains the following participants: users, IoT devices, gateways (fog nodes), controllers, cloud server, smart contract, and the Blockchain, as shown in "Fig. 1". Gateway and controller nodes exist to ease the authentication, store, and retrieve identity data from the Blockchain using the smart contract. Deploying edge nodes in IoT networks provides many advantages, as these nodes are closer to the devices which reduces the latency and also allows us to move the heavy processing tasks from IoT devices to fog nodes. Security concerns like servers denial of service (DOS), distributed denial of service (DDOS) attacks, and data forgery, attacks at the Fog nodes are very likely to happen in traditional networks. However, Fog nodes can detect and analyze any misbehavior and countermeasures these attacks [28]. Using Blockchain as Decentralized storage allows us to tackle scalability and availability limitations that the traditional storage model has.

The following summarizes the role of the different system participants:

- Users: Users are the main customers of the proposed system. Users should register on the cloud server registration form. Upon the completion of user registration, users can register there IoT devices.
- IoT Devices: Each IoT device in the system managed by one gateway. The device owner should initially configure his devices by register the device in the cloud server and get a private key generated. Users

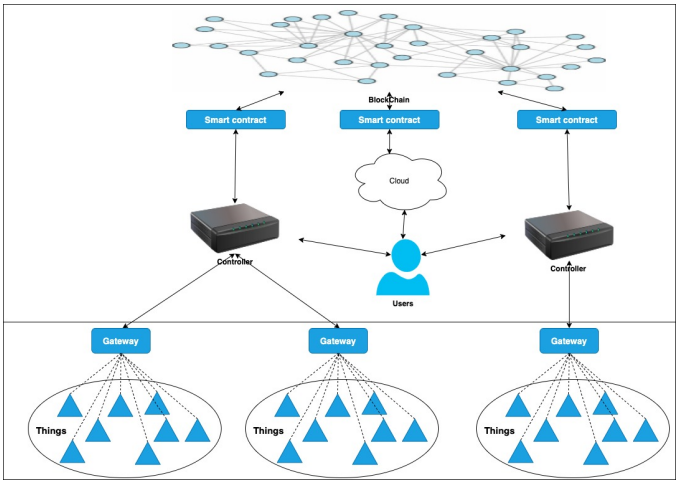

Fig. 1. General architecture.

will add the private key from the previous step into the IoT device. We assume that each IoT device limited by storage and processing capacities, and also IoT device is capable of generating his ECC public key from the ECC private key provided by the owner.

- Gateways: Gateway is a Fog node, each gateway managed by one controller and should be able to manage multiple IoT devices. gateways are used to handle heavy processing that IoT devices cannot handle, as they are closer to the devices, which will reduce network latency between gateways and IoT devices.
- Controllers: Controllers are responsible for registering and managing gateways to the Blockchain, besides playing a central role in the device registration process.
- Cloud Server: In the proposed protocol, there is only one cloud server in this system. Cloud server has an important role in the proposed protocol as it is responsible for deploying the smart contract, creating users, adding user's devices, generating the device's private keys, and registering controller to the Blockchain.
- Smart Contract: In the proposed protocol, there is only one smart contract in this system, which implements the following functions: add users, add gateways, add controllers, add devices to users. Moreover, the smart contract is allowing us to authenticate the requests and add some business logic inside the Blockchain.

The following summarizes all the different steps in the proposed protocol and also, how all the system participants collaborate.

A. User Registration

In this step, the user will register its data in a registration form hosted on the cloud server. During this step, the cloud server sends user data to the smart contract function "addUser". in this step, the cloud server account is the only authorized account to call this smart contract function Fig. 2.

TABLE I. SYMBOLS AND FULL NAMES.

Symbol	Full Name
ID	$Identifier$
DI	$Deviceinfo$
Ku	$Publickey$
Kr	$Privatekey$
N	$Nonce$
Ce	$Certificate$
T	$Accesstoken$
TS	$Timestamp$

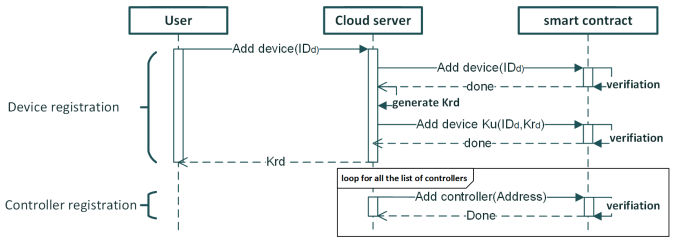

Fig. 2. Cloud server flow.

B. Devices Registration

Every IoT device should be uniquely identifiable [29]. So they could be authenticated autonomously. A pre-embedded identifier will guarantee a unique identity for the IoT device. Device registration will happen in two steps:

1) step 1: During this step, the user should register his own devices on the cloud server registration form. The cloud server will add the user device to the Blockchain using the smart contract function Add device, and in return, the user will get a private key to configure his IoT device. The IoT device should be able to generate an ECC public from the private key provided by the user.

2) step 2: The IoT device sends a registration request to the gateway containing its (Ku_d) device public key. The gateway responses with the gateway public key (Ku_g). Then the device sends (ID_d) (the pre-embedded identifier)along with (DI) device information in JSON-LD format Figure 4 and (N_1) nonce to prevent the replay attack. This nonce also will be used as a challenge to grantee a strong connection authentication between the device and the gateway. This request is encrypted by the gateway public key $E(Kug, IDd||DI||N1)$. A timestamp (TS_1) is a must to prevent the intruder from storing this request and recall it later. The message will be in this form $E(Kuc, IDd||DI||N1||TS1)$. The gateway checks (TS_1) to check if this is a recent request or not. The gateway validates the request internally and sends a registration request to the controller contains $E(Kuc, Kud||IDd||DI||N2)$ along with N_2 as a challenge to authenticate the communication and also to prevent the replay attack. The controller receives the encrypted registration request. Then checks if the device identity exists on the Blockchain using the smart contract. If the device registered by the user, then the controller adds device public key and device information $(Kud||IDd||DI)$ on the Blockchain using the blockchain smart contract. The controller sends back $(Kud||IDd)$ along with (N_2) to the gateway. This message is encrypted by the gateway public key $E(Kug||Kud||IDd||N2)$. The gateway checks the value of

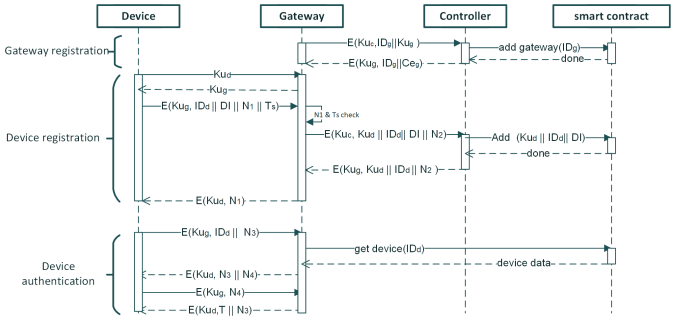

Fig. 3. Messages flow.

```
{
"@context":
 ↪  "http://example.com/contexts/security",
"@type": "Device",
"id": "83d7fdca-2ac4-4869-a3bd-cde2c96d
 ↪  b00f",
"Ku": "0x02f54ba86dc1ccb5bed0224d23f01ed
 ↪  87e4a443c47fc690d7797a13d41d2340e1a",
"issuer": "controller1@controllers",
"issued": "2020-03-01T12:11:17Z",
"claims": [ .... ]
}
```

Fig. 4. Device JSON-LD.

N_2 if it's valid The gateway responses with (ID_d), (Ku_g) to the device $E(Kud, IDd||Kug||N1)$. The IoT devices limited processing resources considered during the registration steps. The messages flow is described In the following "Fig. 3".

C. Gateway Registration

Each gateway requests a public key certificate (Ce_g) from the controller. The request consists of the gateway identifier (ID_g) and its gateway public key (Ku_g) encrypted by controller public key $E(Kuc, IDg||Kug)$. The controller registers the gateway on the Blockchain using the smart contract. The controller responds to this request by validating the gateway identity is valid. Then the controller will add the gateway (ID_g) to the Blockchain using the smart contract function Add gateway after adding the gateway to the Blockchain Controller will generating a certificate for the gateway (Ce_g) and signs it using its private key, (Kr_c) and sends it back along with the gateway (ID_g) controller response should be like this $E(Kug, IDg||Ceg)$. The gateway would authenticate this request if it received the same (ID_g) that sent in the first request. After receiving (Ce_g) the gateway will use this certificate to authenticate itself to the controller.

V. Evaluation and Results

This section evaluates the smart contract functionality and the protocol vulnerability to attacks. The first part focuses on testing smart contract functionality among system participants through Ethereum smart contracts implemented in the Remix IDE. Remix IDE is a tool to implement, deploy, and test the Ethereum smart contract.

The second part presents a security testing simulation for messages protocol between device, gateway, and controller using AVISPA/ HLPSL.

Fig. 5. The result of adding a user successfully when the request sent using the cloud server EA.

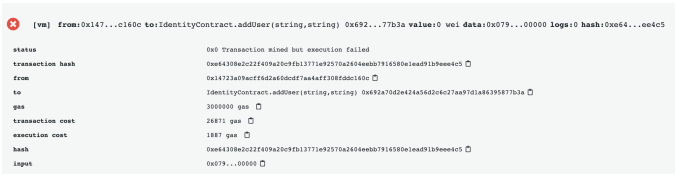

Fig. 6. The result of adding a user failed when the request did not send from the cloud server EA.

A. Smart Contract Evaluation

This step emphasizes on the smart contract interactions among system participants. smart contract implementation is tested using solidity 0.6.1 and Remix IDE.

Four test cases used to cover the most impact function in the smart contract, and these test cases are: 1: Add a controller and add a user using the cloud server (EA) response should be a success 2: Add a controller and add user using (EA) other than the cloud server (EA), the transaction should fail 3: Add gateway using the controller (EA) response should be a success 4: Add gateway using (EA) other than the controller (EA), the transaction should fail . The testing goal is to validate the functionality of the proposed smart contract logic.

During this testing, three Ethereum Addresses (EA) are used. A unique EA assigned to each participant (Cloud server, controller, and gateway).

1) Adding controller and Adding user from authorized EA: In order to add a user mapping using add user function in the smart contract to the Blockchain, a user request should come from the Cloud server EA in order to have a successful event. Fig. 5 showed a successful transaction in Remix when the cloud server EA is used. Also, the controller Id or user Id in the executed function requesting does not exist before. Otherwise, the smart contract will return a duplication error even if the request came from the cloud server address.

2) Adding controller and Adding user from unauthorized EA: If the addition request came from a different EA other than the cloud server EA, the smart contract would return an error message, and operation will fail, as shown in Fig. 6.

Fig. 7. The result of adding a gateway succeeded when the request from a controller EA.

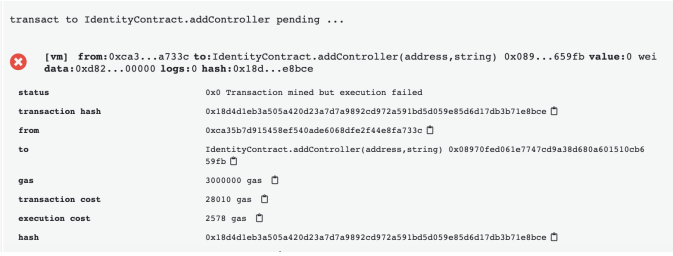

Fig. 8. The result of adding a gateway failed when the request from a non-controller EA.

3) Adding gateway from authorized EA: When attempting to add gateway mapping, smart contract checks if this request comes from the controller EA in order to have a successful event. The smart contract adds the controller EA to a list during the add controller request. This addition allows the smart contract to check if the sender EA exists in the controller list or not to authenticate the request. Fig. 7 shows a successful transaction in Remix when using a controller EA.

4) Adding gateway from unauthorized EA: If the add gateway request comes from a different EA other than the controller's EA, the smart contract will return an error and operation will fail, Fig. 8 shows a failed request sent from a non-controller EA.

B. Protocol Evaluation

The proposed protocol is tested using AVISPA/ HLPSL by simulating the intruder behavior, searching for any insecure channel, encryption efficiency, or weak authentication. This analysis, has the following assumptions: intruder knowledge includes all the public keys, and also intruder is aware of all roles but not the private keys nor device IDs. The main attacks that considered by this analysis are masquerade, man-in-the-middle, and replay attacks. The outcome result from the AVISPA analysis is a safe protocol or not a safe protocol based on the secrecy and weak authentication criteria. This test includes three different steps. In each step, there are specific roles, session knowledge, initial state, and transactions. This protocol has the following steps: (step 1) Gateway registration, (step 2) Device registration, and (step 3) device authentication. In (step 1) there are two roles Gateway and Controller. The predefined goals for this step are the secrecy of $(IDg||T)$ and the strong authentication between the Gateway and Controller. The gateway ID is used as a challenge to authenticate the connection between controller and gateway. In (step 2) there are three roles Device, Gateway, and Controller. Analysis goals are defined to be the secrecy of $(IDd||N1)$ and the strong authentication between Device and Gateway. In (step 3), there are two roles Device and Gateway. Goals are defined to be the secrecy of (T), and also strong authentication between device the controller Connection. This paper selected the ECC cryptography to reduce the overhead in our schema as the key size fits the IoT limited storage and processing capacity. IoT devices should store its identity, private and public keys and also gateway public key $(Kud||Krd||IDd||Kug)$. The device should create a nonce as a challenge to authenticate the gateway. In (step 3) when the device receives the access token (T), the device should check the received nonce.

The result of the AVISPA for the above three steps shows that the proposed protocol is safe, the secrecy and strong authentication criteria are met.

VI. Conclusion

This paper proposed an improved authentication protocol for IoT networks. The proposed protocol took into consideration the limited processing and storage capacities of the IoT devices by moving the heavy processing to the Fog nodes and also using a decentralized identity storage Blockchain. The smart contract functionality is tested using four test cases, and these tests met the expected results. AVISPA results showed that this protocol is immune to network threats as the proposed protocol secures the communications between Devices, Gateways, and Controllers. The functionality of the smart technology gateways reduced the delay and enabled a robost authentication, which surpasses most of the presented authentication protocols. Eventually, identity data are stored in Blockchain using the smart contract. This step removed the overhead of having centric storage for identities because centric storage is a single point of failure. The proposed protocol achieved these goals security, scalability, delay reduction, and splitting processing between fog nodes and devices. By achieving these goals, we made sure that this system is suitable for IoT networks.

References

[1] Lee I, Lee K. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Business Horizons. 2015. pp. 431–440. doi:10.1016/j.bushor.2015.03.008.

[2] Kemp S. Digital 2019: Global Digital Overview — DataReportal – Global Digital Insights. In: DataReportal – Global Digital Insights [Internet]. DataReportal – Global Digital Insights; 31 Jan 2019 [cited 3 Feb 2020]. Available: https://datareportal.com/reports/digital-2019-global-digital-overview

[3] Irfan Saif and Sean Peasley and Arun Perinkolam, "Safeguarding the internet of things: Being secure, vigilant, and resilient in the connected age," 2015, URL: https://dupress.deloitte.com/dup-us-en/deloittereview/issue-17/internet-of-things-data-security-and-privacy.html [Retrieved: 2015-07-27].

[4] M. Weber and M. Boban, "Security challenges of the internet of things," in 2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), May 2016, pp. 638–643.

[5] Commercial National Security Algorithm Suite and Quantum Computing FAQU.S. National Security Agency, January 2016.

[6] Michale Kan, "Chinese firm recalls camera products linked to massive DDOS attack," 2016, URL: http://www.pcworld.com/article/3133962/chinese-firm-recals-cameraproducts-linked-to-massive-ddos-attack.html [Retrieved: 2016-10-24]

[7] Benantar, Messaoud. (2006). Access control systems. Security, identity management and trust models. Access Control Systems: Security, Identity Management and Trust Models. 10.1007/0-387-27716-1.

[8] Digitial Identity in Cyberspace. [cited 2 Feb 2020]. Available: http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall98-papers/identity/white-paper.html

[9] M. Levine and J. Date, "22 million affected by opm hack, officials say," ABC News, July, vol. 9, 2015.

[10] J. Silver-Greenberg, M. Goldstein, and N. Perlroth, "Jpmorgan chase hack affects 76 million households," New York Times, vol. 2, 2014.

[11] T. Gabriel, A. Cornel-Cristian, M. Arhip-Calin and A. Zamfirescu, "Cloud Storage. A comparison between centralized solutions versus decentralized cloud storage solutions using Blockchain technology," 2019 54th International Universities Power Engineering Conference (UPEC), Bucharest, Romania, 2019, pp. 1-5.

[12] Tordera, E. M., Masip-Bruin, X., Garcia-Alminana, J., Jukan, A., Ren, G. J., Zhu, J., Farre, J. (2016). What is a Fog Node A Tutorial on Current Concepts towards a Common Definition. arXiv preprint arXiv:1611.09193

[13] Chen J, Liu Y, Chai Y. An Identity Management Framework for Internet of Things. 2015 IEEE 12th International Conference on e-Business Engineering. IEEE; 2015. pp. 360–364.

[14] Salman O, Abdallah S, Elhajj IH, Chehab A, Kayssi A. Identity-based authentication scheme for the Internet of Things. 2016 IEEE Symposium on Computers and Communication (ISCC). IEEE; 2016. pp. 1109–1111.

[15] van Thuan D, Butkus P, van Thanh D. A User Centric Identity Management for Internet of Things. 2014 International Conference on IT Convergence and Security (ICITCS). 2014. doi:10.1109/icitcs.2014.7021724

[16] M. Trnka and T. Cerny, "Identity Management of Devices in Internet of Things Environment," 2016 6th International Conference on IT Convergence and Security (ICITCS), Prague, 2016, pp. 1-4.

[17] M. Takemiya and B. Vanieiev, "Sora identity: Secure, digital identityon the blockchain," in 2018 IEEE 42nd Annual Computer Software andApplications Conference (COMPSAC). IEEE, Jul. 2018.

[18] Almadhoun, R., Kadadha, M., Alhemeiri, M., Alshehhi, M., Salah, K. (2018). A User Authentication Scheme of IoT Devices using Blockchain-Enabled Fog Nodes. 2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA). doi:10.1109/aiccsa.2018.8612856

[19] D. Li, W. Peng, W. Deng, and F. Gai, "A Blockchain-Based Authentication and Security Mechanism for IoT," in 2018 27th International Conference on Computer Communication and Networks (ICCCN), 2018, pp. 1-6.

[20] P. N. Mahalle, N. R. Prasad, and R. Prasad, "Threshold cryptographybased group authentication (tcga) scheme for the internet of things (iot)," 2014 4th International Conference on Wireless Communications, pp. 1– 5, 2014.

[21] Max Roser, Hannah Ritchie and Esteban Ortiz-Ospina (2020) - "Internet". Published online at OurWorldInData.org. Retrieved from: 'https://ourworldindata.org/internet' [Online Resource]

[22] Kosmatos, E.A., Tselikas, N.D. and Boucouvalas, A.C. (2011) Integrating RFIDs and Smart Objects into a Unified Internet of Things Architecture. Advances in Internet of Things: Scientific Research, 1, 5-12. http://dx.doi.org/10.4236/ait.2011.11002

[23] Kardi A, Zagrouba R, Alqahtani M. Performance Evaluation of RSA and Elliptic Curve Cryptography in Wireless Sensor Networks. 2018 21st Saudi Computer Society National Computer Conference (NCC). 2018. doi:10.1109/ncg.2018.8592963

[24] Hong, H.-J. (2017). From Cloud Computing to Fog Computing: Unleash the Power of Edge and End Devices. 2017 IEEE International Conference on Cloud Computing Technology and Science (CloudCom). doi:10.1109/cloudcom.2017.53

[25] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[26] K. J. O'Dwyer and D. Malone, "Bitcoin mining and its energy footprint," 25th IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014), Limerick, 2014, pp. 280-285.

[27] AVISPA Project. AVISPA Web Tool. At http://www.avispa-project.org/web-interface/.

[28] Bhardwaj, Ketan, Miranda, Joaquin Chung, Gavrilovska, Ada. Towards IoT-DDoS Prevention Using Edge Computing. Conf Proc IEEE Eng Med Biol Soc. 2018; 7.

[29] Chebudie, Abiy Biru and Minerva, Roberto and Rotondi, Domenico. Towards a definition of the Internet of Things (IoT). IEEE Internet Initiative. 2014.