Energy Reports xxx (xxxx) xxx

Contents lists available at ScienceDirect

Energy Reports

journal homepage: www.elsevier.com/locate/egyr

Increasing privacy and security by integrating a Blockchain Secure Interface into an IoT Device Security Gateway Architecture

Marko Šarac [a], Nikola Pavlović [a,*], Nebojsa Bacanin [a], Fadi Al-Turjman [b], Saša Adamović [a]

[a] Faculty of Informatics and Computing, Singidunum University, Danijelova 32, 11000 Belgrade, Serbia
[b] Artificial Intelligence Engineering Dept., Research Centre for AI and IoT, Near East University, Nicosia, Mersin 10, Turkey

ARTICLE INFO

Article history:
Received 24 May 2021
Received in revised form 2 July 2021
Accepted 26 July 2021
Available online xxxx

Keywords:
Security
Internet of Things
Blockchain
Security gateway
Privacy

ABSTRACT

Internet of Things and Blockchain are considered two major technologies. Lower latency and a higher linked system number provide greater flexibility for remote execution of Internet of Things (IoT) applications. It is no secret that IoT devices often have insufficient computing capacity (both in terms of processing power and storage requirements) to support robust protection and encryption algorithms. The Internet of Things is facing many challenges such as poor interoperability, security vulnerabilities, privacy, and lack of industry standards. Cyber-attacks on IoT devices can have an impact on energy trading privacy and security. This paper suggests a method for introducing a basic interface to an IoT device's security gateway architecture along with Blockchain to provide decentralization and authentication. It adds much-needed anonymity and versatility to IoT infrastructure, which is currently lacking. The solution enhances the reliability of data sent to remote services by applying compatible cryptographic algorithms to it before sending it. The solution's benefits include compatibility with all IoT products and the ability to run any cryptographic algorithm on data that can be used for microgrid trading and can be initialized and securely transported over 5G or 6G network infrastructures. As a part of this work, a security procedure has been created that supports every cryptographic algorithm for all IoT devices in the network. In addition, the interface is guarded by the Blockchain technology which eliminates single control authority, records historical transactions performed by the IoT devices and provides a trust between devices.

1. Introduction

IoT devices need a persistent Internet connection to exchange data, making the 5G network an excellent choice in terms of low latency and high data peak speeds (Neves et al., 2017). Current 5G networks can initialize 106 devices per square kilometre with up to 10Mbps per square kilometre and 1 ms round-trip latency, and IoT connects to several computers and devices using wired and wireless networks. In terms of availability, these characteristics of current 5G networks make them an excellent option for IoT applications, but risks must be considered and handled properly.

The concept of Internet of Things and Internet of Energy (IoE) is getting more and more embedded in everyday life. It allows better decision making, easier energy (Devabalaji et al., 2020) transactions and intelligent automatization of distribution (Lu et al., 2020). This means that IoT and IoE will require strong security solutions on all parts of its infrastructure.

One of the most significant challenges in IoT is implementing protection. This paper continues the discussion of the state of IoT security and the issues that it raises. It is based on the authors' previous research paper, which had a significant impact and raised awareness for more stable IoT devices (Pavlović et al., 2021). The devices are also related. As a result, IoT may refer to the interconnection of commonly used electronic devices (Zunino et al., 2020). The potential of the Internet of Things to provide a variety of services has made it the fastest-growing technology. It has had a major impact on the environment and society.

The Internet of Things (IoT) aims to transform how we live today by allowing smart gadgets to do daily chores with minimal human participation. Smart cities, smart homes, smart transportation and infrastructure, and other terms are used to describe the Internet of Things.

The main contribution to this work is:

- The development of a security interface for IoT devices.
- Adding of IP mapping for all devices on security interface.
- Adding of Blockchain to prevent access of third parties to interface, provide trust between devices and increase reliability due to being in the closed decentralized network.

* Corresponding author.
E-mail addresses: msarac@singidunum.ac.rs (M. Šarac), nikola.pavlovic.141@singimail.rs (N. Pavlović), nbacanin@singidunum.ac.rs (N. Bacanin), fadi.alturjman@neu.edu.tr (F. Al-Turjman), sadamovic@singidunum.ac.rs (S. Adamović).

https://doi.org/10.1016/j.egyr.2021.07.078

Please cite this article as: M. Šarac, N. Pavlović, N. Bacanin et al., Increasing privacy and security by integrating a Blockchain Secure Interface into an IoT Device Security Gateway Architecture. Energy Reports (2021), https://doi.org/10.1016/j.egyr.2021.07.078.

- Development of solution in Node.js and test memory usage for AES, DES, Triple DES

Several working groups and business leaders have proposed IoT device standardization, but no solution has been found (Palattella et al., 2013). IoT has generated an excessive demand for protection because of the increasing demand for connected devices and services around the world. For IoT to reach its full potential, it must be protected from bugs and potential attackers. A variety of attacks and threats are increasing in number and complexity daily — either to conduct as an attacker or to be disposed of as a consumer. To provide users with useful performance, the IoT should ensure the suitability and trustworthiness of the processed data.

There is a critical need for such systems to ensure robustness and reliability at the service level, as well as to support protection. Customers' concerns about security and privacy are increasing as they move toward the Internet of Things. Incorporating IoT into the home and workplace raises new security concerns. Customers and suppliers should be aware of the challenge and exercise caution when dealing with protection and privacy issues.

Security challenges come in the form of design practices, lack of standards and regulations. Many privacy issues are coming from the user's agreement to allow vendors to collect their activity on smart devices. This is where Blockchain comes into use. Blockchain technology removes the server which is the centre of the IoT infrastructure. By progressively checking for each transaction, network request, blockchain allows devices to retain current data flow while also improving security and privacy.

By introducing Blockchain to IoT infrastructure, it provides following advantages:

- There is no single control authority.
- IoT devices have built trust between them.
- All actions performed by IoT devices are recorded.
- The data shared by the devices is private.

The following concerns arise because of the introduction of Blockchain to IoT infrastructure:

- Limitation of storage
- Scalability
- Processing time

The storage limitation is tied to the distributed ledger, which is required for all blockchain transactions to be saved into. Scalability issues are linked to adding more IoT devices to decentralized networks which also increases the processing time for activities done by the devices.

Blockchain technology is based on four concepts:

- A peer-to-peer network, all participants use private/public keys to interact with the network. The private key is used to sign transactions and the public key is used as an address on the network.
- Open and distributed ledger, database of all transactions, which is open to everyone.
- Ledger copies synchronization, a way to synchronize ledger across all participants.
- Mining, a way to prevent adding nodes on a chain, because the chain must be valid and ordered.

2. State of the art — related work

The research for the related work is described in the work's continuation. Other researchers have discovered the most prevalent security issues in IoT hubs, as well as the most popular attacks and strategies used against IoT devices. We conduct a real-world experiment to see if work gives more security after the recommended solution is developed. The assessment concludes with a summary of what has been accomplished and recommendations for further work.

Nawir et al. (2016) The key elements associated with IoT systems, their relationships, explained the increasing security issues in the various environments in which they are integrated. These devices are mainly used in home, medical and transportation. To support billions of IoT devices worldwide, wireless community infrastructure needs to be the least convenient in terms of capacity and can be expanded exceptionally, but in various IoT vertical areas. Manage optimally according to the needs of your unique provider (Anon, 2015). Mobile Internet and IoT are the two main ties to the Destiny Cellular Network, providing a vast view of 5G. The 5G generation is defined for the first community to be extensible, versatile, and smartly designed for the second-connected IoT world. (Chvez-Santiago et al., 2015). According to Anon (2014), 5G handles many elements of future lifestyles such as home, work and transportation, and can be characterized by high visitor range density, high connection density and excessive mobility, IoT ecology. Set the basic functions of the system (Mavromoustakis et al., 2016).

This device should be secure and resistant to unauthorized access when used at home. The most frequent attacks and techniques of network attacks to IoT devices are Denial of Service (DoS) Attack (Thakur, 2015), Wormholes (Goyal and Dutta, 2018), Spoofed, alter, or replay network request (Rong et al., 2013), Sybil (Buford et al., 2008).

Attacks on IoT devices can be performed at various network levels. In the following part of the paper, attacks are sorted and described according to the OSI layer of network they are running on.

On physical layer IoT devices can be influenced by jamming or tampering which creates radio interference and exhaustion on IoT devices which can lead to creation of compromised nodes. Two nodes can transmit on same frequency which can lead to collision on Data Link. Network level can be influenced by spoofed altered or replayed routing information, selective forwarding, sinkhole, wormholes (Goyal and Dutta, 2018), sybil (Rong et al., 2013), acknowledgment spoofing. Flooding that generates new requests until the IoT device uses all its resources, and de-synchronization can be model of attacks on Transport layer. On Application layer attackers can operate like the normal user in the IoT system. Attackers can execute malicious activities in that IoT system which can lead to attack on reliability (clock altering, selective data forwarding, and data exaggeration).

Mahmoud et al. (2015b) tried to contribute to a better understanding of the threat. The author explained why IoT devices are so beneficial to attackers. Most IoT devices operate without human interaction, making them physically easily accessible to attackers. These devices also operate using wireless networks to allow attackers to carry out moderate attacks and easily obtain sensitive information. Most devices are unable to support complex security algorithms due to hardware limitations. This paper focused on the challenges surrounding devices and services and outlined the most important Internet of Things security issues. The authors concluded that both end users and vendors need to do a lot of work. It is important to define standards that address the shortcomings of current IoT security mechanisms.

D. Usha et al. (Mahmoud et al., 2015a) provides a comprehensive overview of attacks on all layers of the network. New network protocols (such as IPv6 and 5G) must be implemented to drive security devices to achieve dynamic IoT topology combinations. Most attacks occur at the perception layer, network layer and application layer. Most of the signals transmitted between IoT devices may be interfered with and thus affected. Relay attacks

will take advantage of this layer of confidentiality. Relay attacks can be carried out by changing, copying, or forging the identity information provided by the device. Another type of attack that can be performed on this layer is the time attack. Perform timing attacks by analyzing the time required to perform encryption. The result of this attack is that the attacker can access the encryption key. The attacker can gain physical access to the node and capture all information and data. This is called a node capture attack. At the network layer, the most popular attacks are denial of service (DoS) attacks and man-in-the-middle attacks. Due to the lack of security standards or policies on the Internet of Things, a large number of devices can withstand attacks at the application layer. Different programs and applications have different security algorithms or no security algorithms. The biggest problem here is that different IoT devices need to be compatible with each other. The author concludes that the equipment should use a newer network standard. They proposed an implementation of a smart device smart framework with end-to-end security. New hardware, software, wireless and identification technologies are needed to overcome the challenges of the Internet of Things.

Silex/Brickerbot (Shouran et al., 2019) was discovered in 2017 but appeared again in 2019. The software scans for public internet access and tries to find IoT devices in it. If the IoT device is discoverable, it tries to access it using most common weak login combinations. If it gains access, it deletes all network data on the smart device which makes it unusable unless somebody physically gets access to the device to restart it to factory defaults. The malware has no other purpose but destructive one, making the device unusable.

In 2016 Mirai botnet (Kambourakis et al., 2017) took over 8.4 million IoT devices. The devices were used to perform Distributed Denial of Service (DDoS) attacks. Some actions to find malicious code on devices are performed even today. The problem here is that there is no recorded history of actions performed by devices which makes it even harder to find a malicious device in the network.

Kumar and Mallick (2018) researched what challenges are facing current IoT infrastructure. In the paper authors dealt with privacy and security challenges. They have identified the biggest issues with current infrastructure and provided an overview of them all. With the provided overview authors also provided why Blockchain is needed in the IoT. Some of the sectors where blockchain and IoT can be merged and provide good benefits are Agriculture, Business, Distribution, Energy (Yuvaraj et al., 2017), Food, Finance, Healthcare, Transport and logistics and Smart city. Authors also provided a list of benefits such as tamper proof data, elimination of single control authority, robust, record data of old transactions in smart devices and others.

The motivation for this work comes from the observed problems that exist in all IoT devices. The IoT hub provided by the manufacturer (if any) offers few or no security features. These hubs mainly integrate different IoT devices of the same brand. Other IoT centers are mainly used to observe the IoT devices (smart cameras, walkie-talkies, etc.) in the smart home and display the data they provide on the PC. The solution is a simple interface suitable for any IoT device and network infrastructure. Using blockchain as an additional layer prevents other attackers from accessing smart devices. The main feature of this work is that it supports any encryption algorithm used by remote servers to provide data to IoT devices.

3. Proposed solution

Theoretically, the paper presents a solution that has been developed down to the actual implementation and security evaluation. This solution is based on the following environment:

- Custom home server (hub) for all connected smart devices.
- Using wired connections between the smart device and home servers.
- Adding a layer of security to home server-firewall, serialization of data, compression of data, encryption.
- Using a programming language so the server would be able to run on any device.
- Prevents the smart device from communicating directly to the internet or the internet to communicate directly to the smart device. All communication must be done through the home server.
- Adding Blockchain technology and decentralizing the network. Add distributed ledger to monitor all requests and add an additional layer of security by using blockchain authentication and prevent any requests done by the device to be tempered with.

On Fig. 1. Blockchain logic is included in Home Server. When parsing incoming data, Blockchain validate the data, create new Blocks, and add them to Distributed ledger.

The security of smart devices is the same as the security of wireless networks (Kavianpour and Anderson, 2017). The abuse of the hub device is the same as the abuse of any connected device. The hub connects smart devices to the IP network and has a pre-established trust relationship. It is the same as the security of the wireless network to which the hub's security is connected. Since some smart devices do not support hubs, this security is based on network security. To improve the security of these devices, we have proposed a custom home server (hub) based solution for all smart devices regardless of the support of the hub. This solution consists of a home server, wired or wireless connection to a smart device, and the Blockchain technology. All data sent from smart devices to their remote services will be intercepted and parsed by the server. This means unnecessary leaked information can be removed about the device and properly encrypt the package before sending it to the service. The data from the smart device needs to be parsed and prepared for the remote service in the correct format. To intercept this data, we are using Blockchain technology to monitor each network request done by the node, IoT device. Using a sniffing application such as Wireshark (Iqbal and Naaz, 2019) we can detect which device is sending a request to which service, their IP address, and port, this way we can make sure that the data written in the distributed ledger is correct. All the requests inside a private network are transactions and there is no way for them to be fabricated or changed. Each transaction is saved in Distributed Ledger, a database that can be on the blockchain interface. A blockchain interface could be hosted on any computer and the distributed ledger could be saved on the device, local network server or in case of usage in smart homes where there is no local server a remote database that can be encrypted with strong encryption algorithm and requested to this server can be done using RSA algorithm.

The home server performs the following functions: Obtain information from the smart device; Data should be parsed. Determine that this data is correctly encrypted and transmitted to the remote service (using the Http(s) protocol). Additional features we want on the home server:

- Smart device data monitor for any suspicious requests.
- If possible, using a strong encryption algorithm (Faheem Mushtaq et al., 2017) (only possible if remote service is supporting different encryption standards). This should be possible to activate per smart device in-home network.
- Use Blockchain technology to prevent any tampering with network requests by third parties.
- Add additional authentication via Blockchain to provide trust between IoT devices in the same network.

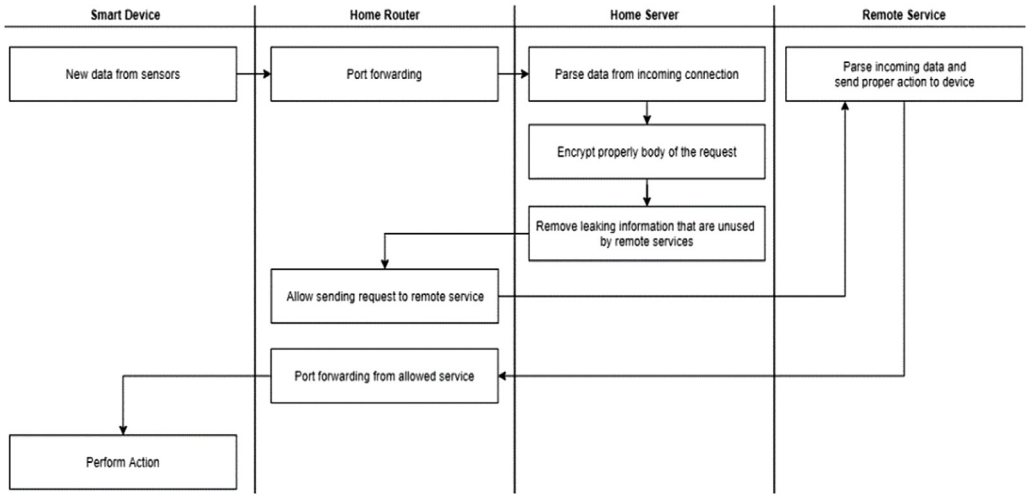

Fig. 1. Proposed solution displayed on activity diagram.

The home server interface should be written in a programming language that can be run on most devices. In solution, Node.js (Sun et al., 2018) is used as a programming language. Node.js has good support for most devices. Some process managers for Node.js such as PM2 have good support for the container approach. This means the home server would be in a container and any attacker would have a hard time connecting to it. PM2 also supports cluster mode. Since Node.js is a single-threaded language cluster mode allows applications to utilize all cores of the CPU allowing applications to be scalable. This greatly increases the performance of the server depending on the number of core CPUs. Each process is created on a new cluster. If an attacker tries to exploit any process on the server, the cluster will destroy the process after a certain amount of time to make sure the server works as intended. Using the home server, the work will prevent the following attacks:

- Man in the middle (Sarma and Barbhuiya, 2019), there will be no way for attackers to directly sniff data from smart devices. The only data they will be able to get is one from the router to the internet. If properly encrypted there will be a very low chance of doing any exploitation.
- Directly connecting to a smart device and doing any exploit on it. All connections from remote to a smart device are forwarded to the home server and then checked if the request is coming from approved sources.
- Devices in local area networks that have no authentication will have a new layer of security based on authentication on the home server. To gain access to any smart house device authentication and authorization on the home server would be needed.

This proposed solution can be furthermore improved by adding the following:

- Filtering allows cloud services that can access a Blockchain network, by allowing certain IP addresses or range of addresses that can access.
- Adding an additional layer of security by implementing an interface that will encrypt/decrypt the data that is leaving the blockchain network.
- Adding a form of caching response from the cloud to prevent requests leaving the blockchain network. If the same request is sent to the cloud, we can use a distributed ledger to provide a smart device with a previous response from the cloud.

4. Security, trust, and solution limitations

As shown in Fig. 1., the proposed solution has four concerns. The first focus is on smart devices. Smart devices use sensors to collect data and process the data necessary to send it to a remote server. Due to the low processing power of this device, the data collected from external sources is poorly encrypted or not encrypted at all. To ensure the security of this data on the Internet, the proposed solution must intercept it. Data interception starts from the second point of interest. The second point of interest is the Blockchain interface. Blockchain interface looks for each network request as a new transaction. Each transaction is saved in the Distributed Ledger. After a new transaction is saved, the request will be forwarded to the remote server.

To process this data from the router, server is capturing it locally. The data that comes from the device has the following request header and request body. The request header has information like request URL, the request method, status code, version of request (HTTP/1.1 or HTTP/2), encoding information, user agent information, authorization information, and content type information. Some IoT Hubs (Cirani et al., 2015) to work correctly send additional information regarding the hub in the header.

Most of the data in request headers are not used by remote service so it can be omitted. The request body has data that is required for remote service to parse. To prevent data leaking, the server is omitting unused data from each request to the remote service. All requests from the server made to the internet are using the HTTP/2 version of the protocol. To further improve the security of each request it is possible to add a layer of encryption for the request body. This means if a remote service has the functionality to use different encryption algorithms, the server can add it here. For example, the server can generate an RSA key pair (Zhou and Tang, 2011) and add a public key on remote service or generate any symmetric key to use with AES, DES, or Triple DES (Bhat et al., 2015). New prepared requests can now be processed and sent to remote service.

The request is sent from the server to the blockchain interface which then forwards it to the internet. The only entry point for any IoT device in the home network is through blockchain interface requests made to the home server. The same goes for another way around. The remote service parses the data sent by the server and returns the relevant action for the device to take. Again, the blockchain interface is forwarding this request to the server. Any request for an IoT device is forwarded to the server. The validity of the request is checked on the server. The server is then answering the following questions:

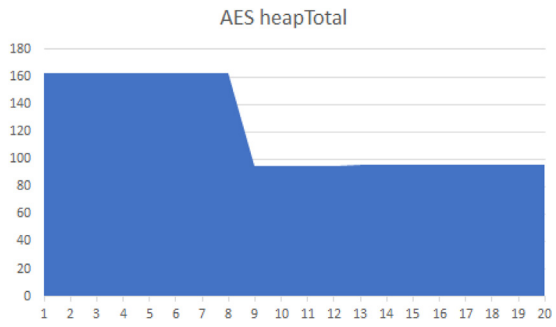

Fig. 2. AES heapTotal memory from 20 processes in MBs.

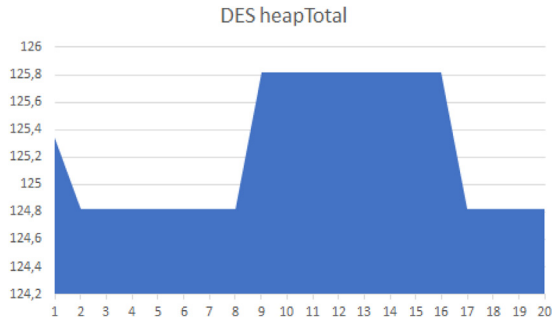

Fig. 3. DES heapTotal memory from 20 processes in MBs.

- Do home servers expect remote service to send a request to an IoT device?
- Do the request body and header contain any suspicious data?

If the server concludes that the request is valid it will be sent to an IoT device in the local area network. After this IoT device will handle the specific action requested by the remote service, as legitimate action.

Memory usage is evaluated using AES, DES, and Triple DES, and here are the results. The measurements are displayed in megabytes. Heap is a memory segment dedicated to storing reference types like objects, strings, and closures. The Heap total represents the total size of the heap used by the server (see Fig. 2).

The home server does not require more than 200 MB of RAM to perform encryption/decryption on smart device data, according to the memory measurements. This means that making of the home server would be inexpensive for mass-production. The lowest memory usage is in the AES algorithm. DES and Triple DES have stable memory usage but are higher than AES (see Fig. 3).

The solution requires a database to save keys for different devices for encryption/decryption purposes. This means if anything happens to the database it will make the solution unusable. This can be solved by using a memory database. When the proposed solution is expecting a response from remote service, and it does not respond it halts the process on the server (see Fig. 4).

Another problem here is linked to the Blockchain interface. By adding the Blockchain to the current IoT infrastructure, we have introduced the problem of scalability. By adding more smart devices to the network, the processing speed lowers. The energy consumption can be furthermore improved by adding smart meters with grid-connected (Shabalov et al., 2021) inverter to provide good performance with low energy consumption cost when upscaling the network.

The most important limitation of all is that most of the code running on smart devices is not open sourced so getting data from

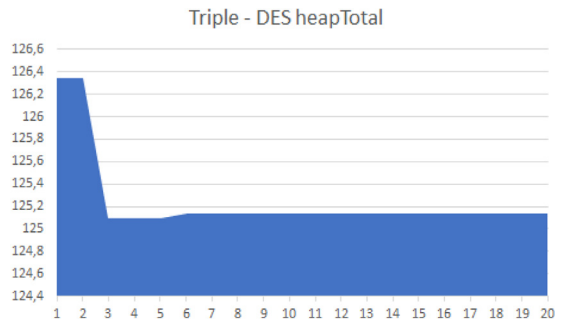

Fig. 4. Triple — DES heapTotal memory from 20 processes in MBs.

Smart Device, parsing, and sending it encrypted to remote service is not possible without direct contact with the manufacturer. Some manufacturers however provide documentation for developers and dashboards where data can be changed, improved, and provided to remote service in a different format.

5. Security evaluation

A class diagram for the proposed solution is presented in Fig. 5. IoT devices send data to an observer. This data can be anything. In this work, Arduino (Andriansyah et al., 2017) is used with sensors for temperature and humidity. Temperature and humidity are measured, and this data is sent to the internet. Before sending it directly to the internet, the Blockchain interface forwards this data to Observer (home server). The observer is parsing the data, performing encryption, and sends it to remote service. Remote service is parsing data, decryption in that process, and based on data it sends a notification to IoT devices to perform certain actions. After authenticating the request, establishing a new transaction, and recording it to the distributed ledger, the Blockchain interface transmits the request to the observer, who decrypts the data and sends it to the IoT device to conduct the required action. In the Class diagram 0 and 1 is used for the Multiplicity. This means that Observer in our case have optional part of it. Sending to remote server can be done or not.

The proposed solution network structure is shown in Fig. 6. It consists of IoT devices, sensors, home server, blockchain interface, network provider, and remote service server.

On Fig. 6. It displays the structure of the proposed solution. Each IoT device is connected to Blockchain infrastructure, and each network request is a transaction. As previously mentioned, the security interface is between the Blockchain interface, and the router and it monitors each request made to the internet. On Fig. 7. Wireshark is used to capture network requests that come from an IoT device to the internet. As shown in the image, the network request body is in plain text. Using the proposed solution, security of the network request body can be much improved. Wireshark has been used for network capture request as a de facto standard for network packet inspection.

The evolution of 5G and 6G network infrastructure is considered an important building block for the integration of IoT devices. We can expect more IoT solutions with this infrastructure in the coming years. Still, the adoption of IoT devices in 5G and 6G networks certainly presents new security challenges and new types of attacks on personal data collected by IoT sensors and devices. This paper proposes flexible use of any IoT device without worrying about the security provided by the IoT device. This solution provides a simple interface that adds the highest security compatibility with the remote service the IoT device is connected to. This solution is meant to provide security compatible with remote services. The encryption algorithm is moved from

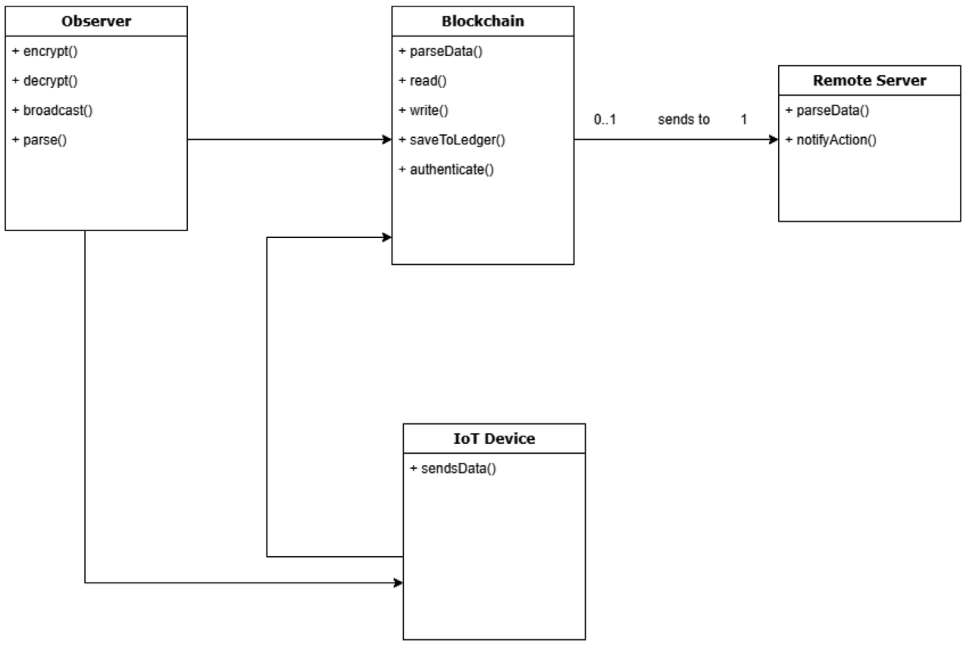

Fig. 5. Proposed solution presented on class diagram.

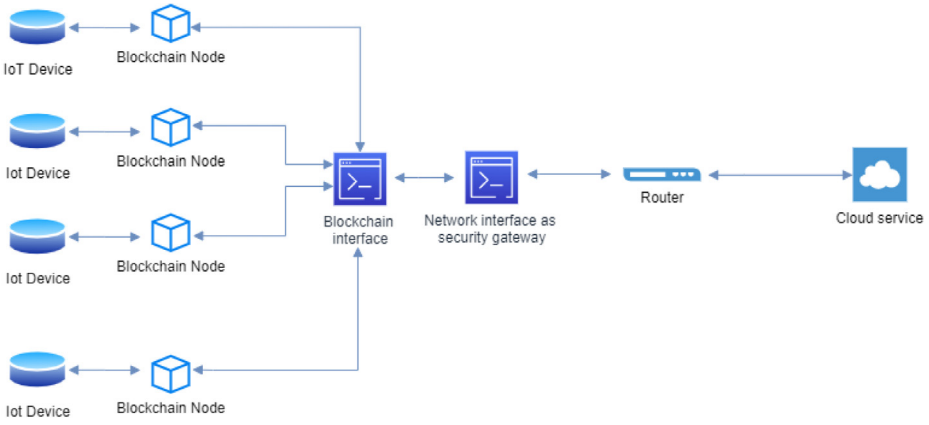

Fig. 6. Blockchain based diagram for the proposed solution.

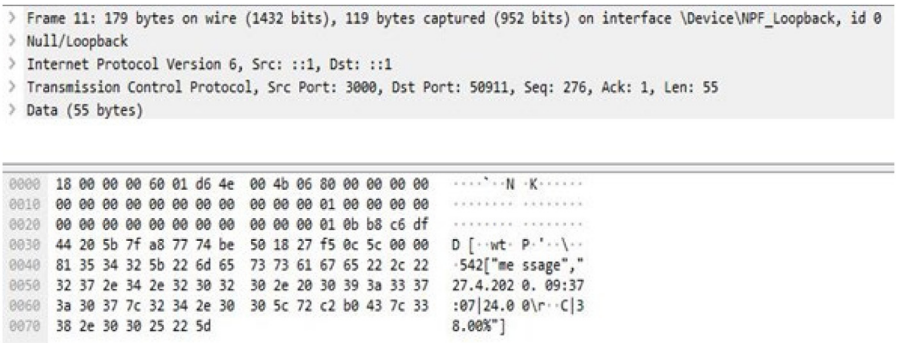

Fig. 7. Wireshark capture of single packet from the proposed solution.

the IoT device to the host server. Servers provide confidentiality, integrity, and availability in a way that is met by the production network. This is done by using existing cryptographic algorithms. This work provides the following:

- Flexibility to use all encryption algorithms.
- Strong security that is moved from IoT device to network layer and device.
- IoT device security is the same as local area network security, server operates at the network layer.
- Intrusion prevention, Check all incoming requests for IoT devices on our local area network.

- Merge of current IoT infrastructure with Blockchain technology.

What needs to be taken into consideration is:

- In order to improve the security of each IoT device in the local area network, IoT device manufacturers must provide a flexible interface to which the device connects. This means that IoT device data sent to the server can be encrypted using one of many modern encryption algorithms.
- IoT device manufacturers must provide a list of IP addresses to which IoT devices are connected. In this way, we can prevent other IP addresses from trying to connect to our IoT device on our local area network.

This solution provides a simple interface that IoT device manufacturers can use to improve the overall security of their devices. The devices can be utilized as is, with no consideration for the network environment (optical, 5G, 6G). The security of smart devices will be considerably enhanced by this way. Smart devices today are vulnerable to different attacks and most smart devices have little or no mandatory security policy. Security is moved to the network layer and the entire data exchange process is enforced by server-to-server end-to-end encryption.

The results of the proposed solutions are that all requests are properly encrypted. New smart devices can be added to the network without any additional changes. The blockchain provides additional layer of security by validating all data that comes from and to the devices.

6. Conclusion and future works

The paper suggests that smart devices' security be improved by limiting direct Internet requests. All requests should be authenticated through the Blockchain interface and, if correct, can be approved. By implementing a simple interface as a security gateway, device manufacturers can add another layer of security protection for Internet communication. This interface can also protect the device from third-party access to the local network that is not allowed by the network rules.

In future work, the server will be optimized to be compatible with a variety of cryptographic algorithms therefore will be able to be used with a wider range of IoT devices. With the proposed merge of the solution, we achieved security of LAN and remote requests. Not only we improved security but got a database (distributed ledger) with a list of all requests written in it. So, if some attack happens, we can debug it from the database and add an additional layer of protection to existing architecture, updating the infrastructure loopholes. In the continuation of this research, we will provide what attacks are possible on current IoT infrastructure and how strong our proposed solution is against them.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Andriansyah, M., Subali, M., Purwanto, I., Irianto, S.A., Pramono, R.A., 2017. e-KTP as the basis of home security system using Arduino UNO. In: 2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT), Kuta Bali, pp. 1-5.

Anon, 2014. IMT: 5G Vision and Requirements. Technical report, International Mobile Telecommunications.

Anon, 2015. Group 4G Americas: 5G Spectrum Recommendations. Technical report, 4G Americas.

Bhat, B., Ali, A.W., Gupta, A., 2015. DES and AES performance evaluation. In: International Conference on Computing, Communication & Automation. Noida, pp. 887–890. http://dx.doi.org/10.1109/CCAA.2015.7148500.

Buford, J., Yu, H., Keong Lua, E., 2008. P2P Networking and Applications. San Francisco, CA, USA.

Chvez-Santiago, R., Szydeko, M., Kliks, A., Foukalas, F., Haddad, Y., Nolan, K., Kelly, M., Masonta, M., Balasingham, I., 2015. 5G: The convergence of wireless communications. Wirel. Pers. Commun. 1–26. http://dx.doi.org/10.1007/s11277-015-2467-2.

Cirani, S., Ferrari, G., Iotti, N., Picone, M., 2015. The IoT hub: A fog node for seamless management of heterogeneous connected smart objects. In: 2015 12th Annual IEEE International Conference on Sensing, Communication, and Networking - Workshops. SECON Workshops, Seattle, WA, pp. 1–6. http://dx.doi.org/10.1109/SECONW.2015.7328145.

Devabalaji, K.R., Thangaraj, Y., Subramaniam, U., Ramachandran, S., Elavarasan, R.M., Das, N., Baringo, L., Rasheed, M.I.A., 2020. A new approach to optimal location and sizing of DSTATCOM in radial distribution networks using bio-inspired cuckoo search algorithm. Energies 13 (18), 4615. http://dx.doi.org/10.3390/en13184615.

Faheem Mushtaq, M., Jamel, S., Hassan Disina, A., Pindar, Z.A., Shafinaz Ahmad Shakir, N., Mat Deris, M., 2017. A survey on the cryptographic encryption algorithms. Int. J. Adv. Comput. Sci. Appl. 8 (11), http://dx.doi.org/10.14569/IJACSA.2017.081141.

Goyal, M., Dutta, M., 2018. Intrusion detection of wormhole attack in IoT: A review. In: 2018 International Conference on Circuits and Systems in Digital Enterprise Technology. ICCSDET, Kottayam, India, pp. 1–5. http://dx.doi.org/10.1109/ICCSDET.2018.8821160.

Iqbal, Haroon, Naaz, Sameena, 2019. Wireshark as a tool for detection of various LAN attacks. Int. J. Comput. Sci. Eng. 7 (5), 833–837. http://dx.doi.org/10.26438/ijcse/v7i5.833837.

Kambourakis, G., Kolias, C., Stavrou, A., 2017. The mirai botnet and the IoT zombie armies. In: MILCOM 2017-2017 IEEE Military Communications Conference. MILCOM, Baltimore, MD, USA, pp. 267–272. http://dx.doi.org/10.1109/MILCOM.2017.8170867.

Kavianpour, A., Anderson, M.C., 2017. An overview of wireless network security. In: 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing. CSCloud, New York, NY, pp. 306–309. http://dx.doi.org/10.1109/CSCloud.2017.45.

Kumar, N., Mallick, P., 2018. Blockchain technology for security issues and challenges in IoT. Procedia Comput. Sci. 132, 1815–1823.

Lu, Q., Zhang, Z., Lü, S., 2020. Home energy management in smart households: Optimal appliance scheduling model with photovoltaic energy storage system. Energy Rep. 6, 2450–2462.

Mahmoud, R., Yousuf, T., Aloul, F., Zualkernan, I., 2015a. Cyber security and internet of things: Vulnerabilities, threats, intruders and attacks. 2015 J. Cyber Secur. Mobil. 65–88. http://dx.doi.org/10.13052/jcsm2245-1439.414.

Mahmoud, R., Yousuf, T., Aloul, F., Zualkernan, I., 2015b. Internet of things (IoT) security: Current status, challenges and prospective measures. In: 2015 10th International Conference for Internet Technology and Secured Transactions. ICITST, London, pp. 336–341. http://dx.doi.org/10.1109/ICITST.2015.7412116.

Mavromoustakis, Constandinos, Mastorakis, George, Batalla, Jordi, 2016. Internet of things (IoT) in 5G mobile technologies. http://dx.doi.org/10.1007/978-3-319-30913-2.

Nawir, M., Amir, A., Yaakob, N., Lynn, O.B., 2016. Internet of things (IoT): Taxonomy of security attacks. In: 2016 3rd International Conference on Electronic Design. ICED, Phuket, pp. 321–326. http://dx.doi.org/10.1109/ICED.2016.7804660.

Neves, Pedro, et al., 2017. Future mode of operations for 5G – The SELFNET approach enabled by SDN/NFV. Comput. Stand. Interfaces 54 (4).

Palattella, M.R., et al., 2013. Standardized protocol stack for the internet of (important) things. IEEE Commun. Surv. Tutor. 15 (3), 1389–1406. http://dx.doi.org/10.1109/SURV.2012.111412.00158, Third Quarter.

Pavlović, N., Šarac, M., Adamović, S., Sarčević, M., Khaleel, A., Maček, N., 2021. An approach to adding simple interface as security gateway architecture for IoT device. Multimedia Tools Appl..

Rong, C., Zhao, G., Yan, L., Cayirci, E., Cheng, H., 2013. Computer and Information Security Handbook, second ed. pp. 345–361. http://dx.doi.org/10.1016/B978-0-12-394397-2.00018-0.

Sarma, R., Barbhuiya, F.A., 2019. Internet of things: Attacks and defences. In: 2019 7th International Conference on Smart Computing & Communications. ICSCC, Sarawak, Malaysia, Malaysia, pp. 1–5. http://dx.doi.org/10.1109/ICSCC.2019.8843649.

Shabalov, M.Y., Zhukovskiy, Y.L., Buldysko, A.D., Gil, B., Starshaia, V.V., 2021. The influence of technological changes in energy efficiency on the infrastructure deterioration in the energy sector. Energy Rep. 7, 2664–2680.

Shouran, Z., Ashari, A., Kuntoro, T., 2019. Internet of things (iot) of smart home: Privacy and security. Int. J. Comput. Appl. 182 (39), 3–8. http://dx.doi.org/10.5120/ijca2019918450.

Sun, H., Bonetta, D., Humer, C., Binder, W., 2018. Efficient dynamic analysis for node.js, 2018. In: 27th International Conference on Compiler Construction. CC 2018, Association for Computing Machinery, New York, NY, USA, pp. 196–206. http://dx.doi.org/10.1145/3178372.3179527.

Thakur, Kutub, 2015. Analysis of denial of services (DOS) attacks and prevention techniques. Int. J. Eng. Res. Technol. 4.

Yuvaraj, T., Ravi, K., Devabalaji, K.R., 2017. Optimal allocation of DG and DSTATCOM in radial distribution system using cuckoo search optimization algorithm. Model. Simul. Eng. 2017, 1–11. http://dx.doi.org/10.1155/2017/2857926.

Zhou, Xin, Tang, Xiaofei, 2011. Research and implementation of RSA algorithm for encryption and decryption. In: Proceedings of 2011 6th International Forum on Strategic Technology. Harbin, Heilongjiang, pp. 1118–1121. http://dx.doi.org/10.1109/IFOST.2011.6021216.

Zunino, Claudio, Valenzano, Adriano, Obermaisser, Roman, Petersen, Stig, 2020. Factory communications at the dawn of the fourth industrial revolution. Comput. Stand. Interfaces 71.