EDITORES:

Manuel A. Serrano - Eduardo Fernández-Medina

Cristina Alcaraz - Noemí de Castro - Guillermo Calvo

Actas de las VI Jornadas Nacionales
(JNIC2021 LIVE)

INVESTIGACIÓN EN ciber segu ridad

Ediciones de la Universidad
de Castilla-La Mancha

Investigación en Ciberseguridad

Actas de las VI Jornadas Nacionales (JNIC2021 LIVE)

Online 9-10 de junio de 2021
Universidad de Castilla-La Mancha

Investigación en Ciberseguridad

Actas de las VI Jornadas Nacionales (JNIC2021 LIVE)

Online 9-10 de junio de 2021
Universidad de Castilla-La Mancha

Editores:
Manuel A. Serrano,
Eduardo Fernández-Medina,
Cristina Alcaraz
Noemí de Castro
Guillermo Calvo

Ediciones de la Universidad
de Castilla-La Mancha

Cuenca, 2021




Edita: Ediciones de la Universidad de Castilla-La Mancha

Colección JORNADAS Y CONGRESOS n.º 34

Esta editorial es miembro de la UNE, lo que garantiza la difusión y comercialización de sus publicaciones a nivel nacional e internacional.

I.S.B.N.: 978-84-9044-463-4
D.O.I.: http://doi.org/10.18239/jornadas_2021.34.00

Hecho en España (U.E.) – *Made in Spain (E.U.)*

Bienvenida del Comité Organizador

Tras la parada provocada por la pandemia en 2020, las VI Jornadas Nacionales de Investigación en Ciberseguridad (JNIC) vuelven el 9 y 10 de Junio del 2021 con energías renovadas, y por primera vez en su historia, en un formato 100% online. Esta edición de las JNIC es organizada por los grupos GSyA y Alarcos de la Universidad de Castilla-La Mancha en Ciudad Real, y con la activa colaboración del comité ejecutivo, de los presidentes de los distintos comités de programa y del Instituto Nacional de Ciberseguridad (INCIBE). Continúa de este modo la senda de consolidación de unas jornadas que se celebraron por primera vez en León en 2015 y le siguieron Granada, Madrid, San Sebastián y Cáceres, consecutivamente hasta 2019, y que, en condiciones normales se habrían celebrado en Ciudad Real en 2020.

Estas jornadas se han convertido en un foro de encuentro de los actores más relevantes en el ámbito de la ciberseguridad en España. En ellas, no sólo se presentan algunos de los trabajos científicos punteros en las diversas áreas de ciberseguridad, sino que se presta especial atención a la formación e innovación educativa en materia de ciberseguridad, y también a la conexión con la industria, a través de propuestas de transferencia de tecnología. Tanto es así que, este año se presentan en el Programa de Transferencia algunas modificaciones sobre su funcionamiento y desarrollo que han sido diseñadas con la intención de mejorarlo y hacerlo más valioso para toda la comunidad investigadora en ciberseguridad.

Además de lo anterior, en las JNIC estarán presentes excepcionales ponentes (Soledad Antelada, del Lawrence Berkeley National Laboratory, Ramsés Gallego, de Micro Focus y Mónica Mateos, del Mando Conjunto de Ciberdefensa) mediante tres charlas invitadas y se desarrollarán dos mesas redondas. Éstas contarán con la participación de las organizaciones más relevantes en el panorama industrial, social y de emprendimiento en relación con la ciberseguridad, analizando y debatiendo el papel que está tomando la ciberseguridad en distintos ámbitos relevantes.

En esta edición de JNIC se han establecido tres modalidades de contribuciones de investigación, los clásicos artículos largos de investigación original, los artículos cortos con investigación en un estado más preliminar, y resúmenes extendidos de publicaciones muy relevantes y de alto impacto en materia de ciberseguridad publicados entre los años 2019 y 2021. En el caso de contribuciones de formación e innovación educativa, y también de transferencias se han considerado solamente artículos largos. Se han recibido para su valoración un total de 86

contribuciones organizadas en 26, 27 y 33 artículos largos, cortos y resúmenes ya publicados, de los que los respectivos comités de programa han aceptado 21, 19 y 27, respectivamente. En total se ha contado con una ratio de aceptación del 77%. Estas cifras indican una participación en las jornadas que continúa creciendo, y una madurez del sector español de la ciberseguridad que ya cuenta con un volumen importante de publicaciones de alto impacto.

El formato online de esta edición de las jornadas nos ha motivado a organizar las jornadas de modo más compacto, distinguiendo por primera vez entre actividades plenarias (charlas invitadas, mesas redondas, sesión de formación e innovación educativa, sesión de transferencia de tecnología, junto a inauguración y clausura) y sesiones paralelas de presentación de artículos científicos. En concreto, se han organizado 10 sesiones de presentación de artículos científicos en dos líneas paralelas, sobre las siguientes temáticas: detección de intrusos y gestión de anomalías (I y II), ciberataques e inteligencia de amenazas, análisis forense y cibercrimen, ciberseguridad industrial, inteligencia artificial y ciberseguridad, gobierno y riesgo, tecnologías emergentes y entrenamiento, criptografía, y finalmente privacidad.

En esta edición de las jornadas se han organizado dos números especiales de revistas con elevado factor de impacto para que los artículos científicos mejor valorados por el comité de programa científico puedan enviar versiones extendidas de dichos artículos. Adicionalmente, se han otorgado premios al mejor artículo en cada una de las categorías. En el marco de las JNIC también hemos contado con la participación de la Red de Excelencia Nacional de Investigación en Ciberseguridad (RENIC), impulsando la ciberseguridad a través de la entrega de los premios al *Mejor Trabajo Fin de Máster en Ciberseguridad* y a la *Mejor Tesis Doctoral en Ciberseguridad*. También se ha querido acercar a los jóvenes talentos en ciberseguridad a las JNIC, a través de un CTF (Capture The Flag) organizado por la Universidad de Extremadura y patrocinado por Viewnext.

Desde el equipo que hemos organizado las JNIC2021 queremos agradecer a todas aquellas personas y entidades que han hecho posible su celebración, comenzando por los autores de los distintos trabajos enviados y los asistentes a las jornadas, los tres ponentes invitados, las personas y organizaciones que han participado en las dos mesas redondas, los integrantes de los distintos comités de programa por sus interesantes comentarios en los procesos de revisión y por su colaboración durante las fases de discusión y debate interno, los presidentes de las sesiones, la Universidad de Extremadura por organizar el CTF y la empresa Viewnext por patrocinarlo, los técnicos del área TIC de la UCLM por el apoyo con la plataforma de comunicación, los voluntarios de la UCLM y al resto de organizaciones y entidades patrocinadoras, entre las que se encuentra la Escuela Superior de Informática, el Departamento de Tecnologías y Sistemas de Información y el Instituto de Tecnologías y Sistemas de Información, todos ellos de la Universidad de Castilla-La Mancha, la red RENIC, las cátedras (Telefónica e Indra) y aulas (Avanttic y Alpinia) de la Escuela Superior de Informática, la empresa Cojali, y muy especialmente por su apoyo y contribución al propio INCIBE.

Manuel A. Serrano, Eduardo Fernández-Medina
Presidentes del Comité Organizador
Cristina Alcaraz
Presidenta del Comité de Programa Científico
Noemí de Castro
Presidenta del Comité de Programa de Formación e Innovación Educativa
Guillermo Calvo Flores
Presidente del Comité de Transferencia Tecnológica

Índice General

Comité Ejecutivo

Juan Díez González	INCIBE
Luis Javier García Villalba	Universidad de Complutense de Madrid
Eduardo Fernández-Medina Patón	Universidad de Castilla-La Mancha
Guillermo Suárez-Tangil	IMDEA Networks Institute
Andrés Caro Lindo	Universidad de Extremadura
Pedro García Teodoro	Universidad de Granada. Representante de red RENIC
Noemí de Castro García	Universidad de León
Rafael María Estepa Alonso	Universidad de Sevilla
Pedro Peris López	Universidad Carlos III de Madrid

Comité Organizador

Presidentes del Comité Organizador

Eduardo Fernández-Medina Patón	Universidad de Castilla-la Mancha
Manuel Ángel Serrano Martín	Universidad de Castilla-la Mancha

Finanzas

David García Rosado	Universidad de Castilla-la Mancha
Luis Enrique Sánchez Crespo	Universidad de Castilla-la Mancha

Actas

Antonio Santos-Olmo Parra	Universidad de Castilla-la Mancha

Difusión

Julio Moreno García-Nieto	Universidad de Castilla-la Mancha
José Antonio Cruz Lemus	Universidad de Castilla-la Mancha
María A Moraga de la Rubia	Universidad de Castilla-la Mancha

Webmaster

Aurelio José Horneros Cano	Universidad de Castilla-la Mancha

Logística y Organización

Ignacio García-Rodriguez de Guzmán	Universidad de Castilla-la Mancha
Ismael Caballero Muñoz-Reja	Universidad de Castilla-la Mancha
Gregoria Romero Grande	Universidad de Castilla-la Mancha
Natalia Sanchez Pinilla	Universidad de Castilla-la Mancha

Comité de Programa Científico

Presidenta

Cristina Alcaraz Tello	Universidad de Málaga

Miembros

Aitana Alonso Nogueira	INCIBE
Marcos Arjona Fernández	ElevenPaths
Ana Ayerbe Fernández-Cuesta	Tecnalia
Marta Beltrán Pardo	Universidad Rey Juan Carlos
Carlos Blanco Bueno	Universidad de Cantabria
Jorge Blasco Alís	Royal Holloway, University of London
Pino Caballero-Gil	Universidad de La Laguna
Andrés Caro Lindo	Universidad de Extremadura
Jordi Castellà Roca	Universitat Rovira i Virgili
José M. de Fuentes García-Romero de Tejada	Universidad Carlos III de Madrid
Jesús Esteban Díaz Verdejo	Universidad de Granada
Josep Lluis Ferrer Gomila	Universitat de les Illes Balears
Dario Fiore	IMDEA Software Institute
David García Rosado	Universidad de Castilla-La Mancha
Pedro García Teodoro	Universidad de Granada
Luis Javier García Villalba	Universidad Complutense de Madrid
Iñaki Garitano Garitano	Mondragon Unibertsitatea
Félix Gómez Mármol	Universidad de Murcia
Lorena González Manzano	Universidad Carlos III de Madrid
María Isabel González Vasco	Universidad Rey Juan Carlos I
Julio César Hernández Castro	University of Kent
Luis Hernández Encinas	CSIC
Jorge López Hernández-Ardieta	Banco Santander
Javier López Muñoz	Universidad de Málaga
Rafael Martínez Gasca	Universidad de Sevilla
Gregorio Martínez Pérez	Universidad de Murcia

David Megías Jiménez	Universitat Oberta de Cataluña
Luis Panizo Alonso	Universidad de León
Fernando Pérez González	Universidad de Vigo
Aljosa Pasic	ATOS
Ricardo J. Rodríguez	Universidad de Zaragoza
Fernando Román Muñoz	Universidad Complutense de Madrid
Luis Enrique Sánchez Crespo	Universidad de Castilla-La Mancha
José Soler	Technical University of Denmark-DTU
Miguel Soriano Ibáñez	Universidad Politécnica de Cataluña
Victor A. Villagrá González	Universidad Politécnica de Madrid
Urko Zurutuza Ortega	Mondragon Unibertsitatea
Lilian Adkinson Orellana	Gradiant
Juan Hernández Serrano	Universitat Politécnica de Cataluña

Comité de Programa de Formación e Innovación Educativa

Presidenta

Noemí De Castro García	Universidad de León

Miembros

Adriana Suárez Corona	Universidad de León
Raquel Poy Castro	Universidad de León
José Carlos Sancho Núñez	Universidad de Extremadura
Isaac Agudo Ruiz	Universidad de Málaga
Ana Isabel González-Tablas Ferreres	Universidad Carlos III de Madrid
Xavier Larriva	Universidad Politécnica de Madrid
Ana Lucila Sandoval Orozco	Universidad Complutense de Madrid
Lorena González Manzano	Universidad Carlos III de Madrid
María Isabel González Vasco	Universidad Rey Juan Carlos
David García Rosado	Universidad de Castilla - La Mancha
Sara García Bécares	INCIBE

Comité de Transferencia Tecnológica

Presidente

Guillermo Calvo Flores	INCIBE

Miembros

José Luis González Sánchez	COMPUTAEX
Marcos Arjona Fernández	ElevenPaths
Victor Villagrá González	Universidad Politécnica de Madrid
Luis Enrique Sánchez Crespo	Universidad de Castilla – La Mancha

COMUNICACIONES

Sesión de Investigación A1:
Detección de intrusiones y gestión de anomalías I

http://doi.org/10.18239/jornadas_2021.34.01

Distributed Architecture for Intrusion Detection in IoT Networks using Smart Contracts

Rafael Z. A. da Mata*, Francisco L. de Caldas Filho†, Lucas M. C. e Martins‡,
Fábio L. L. de Mendonça§, and Rafael T. de Sousa Jr.¶
Cyber Security INCT Unit 6, Electrical Engineering Department, University of Brasilia, Brasilia, Brazil
e-mails: {rafael.zerbini} @uiot.org, {francisco.lopes, lucas.martins, fabio.mendonca}@redes.unb.br, {desousa} @unb.br
ORCID: * 0000-0002-5246-8858, † 0000-0001-5419-2712, ‡ 0000-0001-6436-7408,
§ 0000-0001-7100-7304, and ¶ 0000-0003-1101-3029

***Abstract*—DDoS attacks against distributed networks of IoT devices and applications are increasing. In this scenario, countermeasures must also use distributed security means. This paper proposes a distributed architecture of an intrusion detection system for IoT networks using smart contracts in blockchain. The proposed architecture supports interaction mechanisms between the local controllers using smart contracts to distribute security rules among the different devices on the IoT network. To validate the proposal, this paper presents the assessment of parameters required to ensure an acceptable level of reliability in sharing security rules.**

***Index Terms*—IoT security, intrusion detection, smart contracts, blockchain**

Tipo de contribución: *Investigación original*

I. Introduction

The number of Internet of Things (IoT) devices has grown exponentially over the years. According to a survey presented by [1], in 2015 there were 4.9 billion connected IoT devices and the forecast is that the number of connected devices in 2020 would be 25 billion, an increase of over 500% in just five years. To facilitate the configuration of these devices for end-users, manufacturers often use standard access passwords to configure these elements, thus making them vulnerable to unauthorized access by third-parties [2] thus creating the need for security mechanisms that work on resource-constrained devices [3].

This loophole allows these devices to be used for distributed denial of service (DDoS) attacks as described in [4], turning them part of botnets networks.

There are several security mechanisms to identify whether IoT devices are part of a botnet and to carry out malicious traffic mitigation actions [5], [6], [7]. The mitigation of malicious traffic can occur directly on the device, which identifies abnormal situations in its operation and takes actions to perform corrections, or on the network layer by using firewalls and Intrusion Prevention Systems (IPS) capable of recognizing abnormal situations and blocking traffic. Mitigation directly on the device involves the application of Host-Based Intrusion Detection System (HIDS), where an application running on the device identifies abnormal situations in its processes, on network ports, or in system files and acts to correct the fault.

This method stops the attack at the source, avoiding overloading the network infrastructure. However, it has its limitations:

- IoT devices have low computational power, hampering the execution of verification programs;
- The number of IoT devices grows exponentially making it hard and impracticable to apply security rules to each of them.

The model proposed by the previous work develops a HIDS in which the fault checking rules are configured on a controller in the cloud. The final IoT devices carry out periodic verification to check the need to include new rules in their own table and to take actions to solve problems included by the administrator in these rules. The system was adapted to be lightweight and run on devices with low computational power, being successfully tested on single-board computing (SBCs), such as Raspberry Pi.

However, this model has a dependence on the controller installed in cloud computing resources to be able to serve a large number of devices. Local networks or environments with a large volume of data should always check for new rules on the Internet, making the use of link more expensive and not allowing rules to be updated when there is no Internet connection available. The rules should also be entered into the cloud controller.

The model proposed in this work aims to solve some deficiencies presented in the previous work by creating a defense system associated with local controllers, in which IoT devices search for updated information directly from these local ones. The update of the rules that will be replicated to the devices does not occur only in the device-cloud model, but point-to-point, allowing that rules created and successfully validated in other environments by their local controller can be replicated, creating an always up-to-date federated environment.

To ensure that communication between the controllers occurs safely and only between controllers that are part of the requested federation, an environment was developed in this work where controllers exchange rules with each other using private smart contracts running in a public blockchain network, such as that described in [8].

This paper proposes a HIDS solution distributed for IoT networks. In order for organizations (local controllers of different networks) to share specific rules with other organizations, a solution based on smart contracts in a blockchain environment is proposed. The main advantages of this architecture are consensus on adding rules to the system, inviolability of the rules in the system, authentication in the

exchange of information, and complete audit.

In addition to this introduction, Section II presents the basis of the concepts discussed in this article and Section III point correlated works out and highlights their differences. Section IV describes the proposal of this paper, including its architecture and its description, while Section V presents and discusses the security analysis of shared rules and, finally, in Section VI, the conclusion and possible future work are presented.

II. Theoretical Foundation

Host-Based Intrusion Detection System, or HIDS, is a software traditionally used to perform monitoring routines aimed at detecting intrusion in storage systems [7]. Monitoring, in traditional HIDS's such as those studied by [9], focuses mainly on metric analyzes such as writing to disk and memory, repeated access to certain ports, entry, and exit of processes, in addition to others considered anomalous, as identified by [10]. In the context of IoT networks, there is a need for HIDS's that maintain the analysis and detection profile, but that also keep reduced computational cost, avoiding an overload in the system as shown by [11].

The existence of a single point of failure in IoT architectures is a negative aspect widely discussed, as highlighted by [12] and [13]. As an alternative to this problem, several studies have already made efforts to decentralize the distribution of information, including concerning security rules and for this reason have suggested the use of blockchain with its blocks joined by encryption [14], where the later block has the cryptographic hash of the previous block. The main role of each block is to store records of various transactions, such as changing security rules or a cryptocurrency transfer.

This approach using blockchain is considered advantageous, as seen in [15], because it offers mechanisms that solve problems such as the single point of failure, given the use of distributed architecture typical of blockchain architectures [16], [17]. Another relevant point, also highlighted by [14], is the consensus that is defined by the author as the judgment that each node belonging to the blockchain has the same block sequence. The majority vote defines the veracity of the information contained in the block under analysis.

Regarding the stored information in blockchain, like the aforementioned security rules, one of the alternatives is smart contracts that is defined by [18] as software with deterministic behavior executed in distributed networks whose main function is to mediate between two interested nodes in the exchange of information contained in blockchain. The use of smart contracts has gained much recognition due to its ability to transfer assets in the form, mainly, of cryptocurrencies. Another relevant definition is given by [19] which conceptualizes smart contracts as programs that execute correctly without the intervention of a trusted authority and cites Ethereum as responsible for implementing the smart model contracts currently adopted and also the consensus model applied by it, which is very robust due to it's verification scheme that only allows registration in the blocks for transactions considered valid [20].

III. Related Works

Given the expansion of IoT networks and the continuing need to provide security for these networks and their systems, several solutions using HIDS and blockchain have already been proposed. The review by [21] addresses the main challenges involved in intrusion detection, in particular:

- The problem of data sharing due to distrust between involved parties and also the possibility of reducing the amount of information shared by the same parties due to concerns about privacy, thus reducing the training optimization of detection algorithms;
- The use of a central server that provides trust management, becoming increasingly complex as the organization grows, thus increasing the possibility of internal attacks where nodes belonging to the organization authorize network access for external attackers.

Aiming at solving problems presented by [21], the project developed in this article makes use of blockchain to intensify mutual trust between the parties involved in sharing information and also to favor auditing and inviolability of them, in addition to being implemented in a distributed network to provide more robust trust management, from the point of view of the controllers, since it does not have a single central server as a single point of failure. In the scenario presented in the article, the referred information refers to the exchange of security rules between controllers and nodes.

In the context of traditional IoT infrastructures, [13] presents the distrust between system nodes and the existence of a single point of failure as the two main obstacles to continuous security management. The authors suggest, as a solution, the use of a distributed architecture using blockchain to store user interactions with the IoT environment so that these interactions are persisted in the form of blocks representing the history of the node or user and for this an encrypted token is used to guarantee the legitimacy of the user in question. Unlike the [13] proposal, which uses blockchain to store node history, our proposal uses smart contracts to propagate and store rules on the blockchain network. In addiction to this, our proposal was designed in the form of a distributed network whose validation of the information disseminated by the controllers is done through consensus mechanisms.

SVELTE is an intrusion detection system for IoT networks based on 6LoWPAN protocol proposed in [22], by using a hybrid of signature detection and anomaly detection based approach to perform intrusion detection. However, the system is designed to detect mostly routing attacks such as sinkhole attack, and the selective-forwarding attacks. The work of Surendar and Umamakeswari [23] also proposes a system for the 6LoWPAN protocol but using fewer resources than SVELTE, with a lower packet dropping ration and a more significant number of nodes into the evaluation. Our proposed solution is a novel detection with constrains and improved the shortcoming from SVELTE and INTI.

The work presented in [24] designed a HIDS, wich combines the advantages of Signature Intrusion Detection System (SIDS) and Anomaly-based Intrusion Detection System (AIDS). They also show that SIDS have a low false-

positive rate and show that the hybrid combination of both techniques presents a good accuracy compared to each one of their own. They were also preoccupied with the high energy consumption from the AIDS running all the time, so they used a mechanism only to activate the AIDS when a new attack's signature is expected to occur, which is verified by a SIDS. Their solution is a significant cost benefit between accuracy and energy consumption. We propose a different solution, mainly because our IDS runs in the IoT device.

Khraisat et al. work presented in [25] also proposed a hybrid IDS using signature and anomaly detection, combining a C5 classifier and One-Class Support Vector Machine classifier. Their work aimed to detect known vulnerabilities and zero-days with a high detection accuracy and a low false-alarm rate at the same time. Their model was tested against the Bot-IoT dataset, which includes legitimate IoT network traffic and several types of attacks, their results show a higher detection rate and a lower false-positive rate when compared to SIDS or AIDS techniques individually. We propose only the signature approach and our proposal is executed on the IoT device.

Diro and Chilamkurti's work described in [26] states that many zero-day attacks keep surging due of the many new protocols focused on IoT and most of these attacks are variants of well-known malwares, indicating that even machine learning models don't have a good response against these new attack's variants. Based on that, they proposed a Deep Learning based approach, in which the model would be resilient to small mutation or new attacks since deep learning introduces self-taught and compression capabilities. They showed that their approach was more effective in attack detection. Their approach also was created to work in a distributed environment, and their experiments showed that it was superior than the centralized detection system.

The paper [27] reports the growth of botnet networks related to the increasing number of IoT devices that have security breaches and are included in botnets such as the cited Mirai. However, this work does not address security measures to mitigate such attacks.

In [7], authors show the high frequency of DDoS attacks on IoT networks and cites the need to implement countermeasures that are distributed on the network to offer more effective coordination of IoT nodes. Their presented solution is a HIDS whose main function is to protect the backbone of the IoT network. The proposed HIDS is designed with conventional functionalities such as the authentication system using user and password, search for signatures of known attacks, verification of resource allocation, active processes, open service port and active connections, and as a differential offers the possibility to interact with your HIDS Controller to manage intrusion detection actions distributed over the network in DDoS attack situations. In our proposal presented in this paper, there is more than one provider, different from the scenario proposed by [7]. The main advantages of having more than one rules provider is the speed at which they are broadcast over networks, thus offering a faster response to security incidents such as DDoS and zero day cases.

In [5], a proposal is made for a subscription HIDS system to detect attacks and vulnerabilities in devices that want to connect to IoT networks through HIDS agents for IoT devices that perform the tests determined by the rules. The test result is compared to an expected result and, if it is outside of these parameters, the safety rule is executed and the HIDS controller is notified. The HIDS controller is responsible for managing HIDS agents in the distribution and updating of rules, analysis of alerts, treatment of threats and definition of premises. The scenario presented by [5] has a HIDS controller responsible for accessing the remote database to propagate the rules on the IoT network, different from our proposal that aims to implement a distributed network in which there is no dependency on a single node for spreading the rules to decrease the response time, especially in attack situations such as the aforementioned DDoS.

Finally, the authors suggest the use of blockchain as a way to solve a few challenges such as improving the security and privacy of information, increasing the reliability of the service through reputation systems, negotiating transactions, and dispute management. Our proposal also has a mechanism of reputation system similar to that of the proposal due to the distributed architecture of the rules which also contributes to the aspects of reliability with regard to the degree of confidence of each rule that is disseminated by the network.

IV. Proposed Architecture

The solution proposed in this work is composed of IoT devices that are capable of running the HIDS instance developed in the previous work and remote controllers, in which the security signatures that the final devices need to obey are registered. The final controllers can exchange rules with each other, allowing a federated system in which anomalous behaviors identified in one controller are passed on to the others, allowing the end devices to react to security breaches in a co-ordinated and decentralized manner according to the rules that are propagated by your parent company.

Periodically, the end devices consult remote controllers to find out if there are new rules to be saved in their database. This behavior is similar to anti-virus [28] systems. The possibility of rules that will be registered at the controller and replicated to the final devices are numerous, from the analysis of improper queries to suspicious DNS addresses as in [29], to the verification of any suspicious process as defined in previous work.

The process of exchange rules between controllers is done through a smart contract hosted on the Ethereum [20] blockchain. The rules in the smart contract follow the structure defined below.

- *name*: rule name;
- *id*: unique rule identifier;
- *createdAt*: creation date;
- *premisse*: value considered correct for a given condition or characteristic of the system;
- *testCase*: evaluation code to verify characteristics or conditions on the devices, and returns the result for verification;
- *action*: if the result of the case test is different from the value defined in the premise, the defined action is executed;

- *approvals*: nodes that marked rules as approved, nodes can revoke their votes later, and its added to a subfield called *revoke*;
- *denies*: number of nodes that marked rules as denied, the node also need to provide a reason for denying the rule;

A rule is a block of information that helps the HIDS agent to take predefined actions. This information block has the fields that are shown in Fig. 2 and are described below:

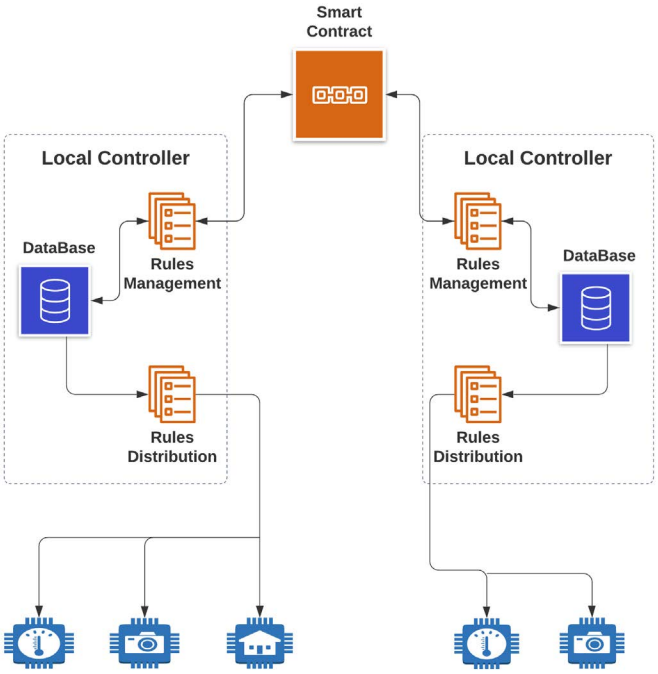


Fig. 1: Distributed Architecture


```
{
  "id": 1,
  "name": "os_name",
  "created_at": "2020-08-10T12:00:00",
  "premise": "Linux",
  "action": "print(\"System is not supported.\")\nraise System exit",
  "test_case": "import platform\noutput = platform.system()",
  "approvalls": [
    {
      "address": "0xc4aEb20798368C48B27280847E187BB332b9bC77"
    },
    {
      "address": "0x5A0b54d5dc17e0AADC383d2DB43b0A0d3e029c4C",
      "revoke": "Wrong premisse output"
    }
  ] ,
  "denies": [
    {
      "address": "0xd4aFb20798742C48B27280847E187BB332b9bC77",
      "reason": "Wrong premisse output"
    }
  ]
}
```


Fig. 2: Example of security rule scheme.

As soon as each node accesses a rule in the smart contract, it has the option to mark the rule as approved or denied, based on its security measures. In situations where more than half of the nodes reject a specific rule, it is marked as invalid and can no longer be accessed by other nodes. As long as the previous condition is not met, nodes can access the rule. Each node is responsible for choosing the number of approvals necessary for the rule to be considered valid for the same.

This architecture brings decentralization in the process of sharing rules between devices on different networks, it also has the advantage of having a form of consensus, in which a node can validate a rule based on other nodes validation. Another advantage is scalability since the largest amount of us offers more rules to distribute and a greater guarantee that rules are safe.

Also, the solution offers flexibility in the implementation of the rule control for each network, since the rules only need to follow a defined pattern when they will be shared for the entire network. Thus, a node that accesses a specific rule on the local network can modify it to meet its needs.

A. HIDS Agent

Each IoT device has a HIDS agent that is responsible for receiving the rules from the controller, saving them to its local database, and executing the rule. After rule execution, the device generates a report that is sent to the controller. In this report, the device informs the results of the case test and, if an action has been performed, it also reports whether it was performed successfully. Reports generated by the agent allow the administrator to keep updated on the status of the network, investigating possible vulnerabilities.

B. Smart Contract

A smart contract is an automatic execution contract whose terms of the contract between different parties are created via code. The agreements contained therein exist in a decentralized and distributed blockchain network. The code controls execution and transactions are traceable and irreversible.

Smart contracts allow reliable transactions and agreements to be carried out between anonymous and disparate parties, without the need for a central authority, legal system, or external enforcement mechanism. The smart contract that stores the rules were developed using the Ethereum blockchain.

The implemented smart contract has three main functions accessed by the nodes:

- *registerApproval*: this function is responsible for registering the approval of each node, the function stores the node address;
- *registerDeny*: this function is responsible for registering the rule deny from each node, the function store the node address and information from the node about the reason for the denial;
- *revogueApproval*: this function is responsible for revoking a previous approval from a node, the node must inform the reason to call a revoke from his vote and all nodes that approved the rule are notified about the revoke, and can also call the function under the same pretense. The revoked votes are marked as revoked in the approval list and added to the deny list.

The smart contract is published by the creator of the rule that is going to be distributed. At any moment any node can consult the numbers of approvals or denies from a rule and

also see the reason for revokes, in case the node wishes to fix the issues itself.

C. Rules Management

The rules that will be executed by HIDS are defined in their entirety at the parent company. The controller can operate within a hierarchical cloud environment, in which the rules registered with the controller are copied to the final devices, with one controller serving all of the final IoT devices. This model has advantages such as simplicity of implementation, however, it presents points of failure that deserve attention, they are:

- The unavailability of communication with the cloud server makes it impossible to send new rules;
- There is a single cloud controller which if is compromised can affect all end devices;
- Depending on the distance between cloud servers and end devices, latency can compromise the exchange of rules and delay reactions to security locks on end devices.

The model proposed in this work, as can be seen in Fig. 1, uses a smart contract system responsible for distributing security rules to controllers in different networks who are responsible for managing, persisting in their own database, and distribute these same security rules to the local devices with which you have a direct connection acting as the default gateway. In this way, there is a considerable reduction in latency, and each end device can operate without a direct connection to the Internet.

The management of the rules is carried out by the network administrator so that he has total autonomy over creating, deleting, updating, and reading the rules. This service is also responsible for informing which rules should be shared with other controllers via smart contract and which have autonomy only locally. In the rules management service, the administrator also checks the rules received from other controllers, using a smart contract, and decides whether they should be applied to their rule base. This service is also responsible for activating the function in the smart contract, validating or not the rule provided by the network.

D. Rules Distribution

With each update or creation of rules by the administrator, the rule distribution service is triggered and aims to distribute the new rule to the devices, according to the definition made by the administrator of which devices should receive the rule.

Confidentiality in the exchange of information is guaranteed by the use of encryption, thus preventing systems that analyze the contents of TCP/IP packets or metadata from obtaining success in obtaining information, as demonstrated in [30]. For this, the exchange of messages between the controller and end devices is performed using SSL so that, being initiated by a TLS handshake [31], the rules are provided to the end device when the session is granted to the device.

V. Security Analysis of Shared Rules

This section assesses the security of the rules shared in the smart contract, considering the research question on how many approvals are needed on a rule to ensure that a rule is secure.

To understand the research question, it is interesting to consider the following scenario: a controller sends a dishonest rule, using the smart contract, and if other controllers cooperate with the dishonest node, the rule can generate vulnerabilities on the devices that receive the rule. That is why it is important to establish a minimum security threshold on the received rule to ensure the security of the networks.

To validate the consensus of the rules, a statistical study was carried out to assess the probability that the number of approvals is greater than the number of denials, given a certain number of confirmations imposed by a node.

For this purpose, tests were carried out following a binomial model to simulate nodes approving or denying transactions. The binomial models used have two probabilities, p, that a node approves a rule, which are $p = 0.6$ and $p = 0.8$, and two probabilities of rejecting a rule, q, $q = 0.4$ and $q = 0.2$ respectively. For the tests, different node values were used, which are called N, and the values used were $N = 10$, $N = 50$ and $N = 100$. The minimum values chosen for approval, k, were $N/8$, $N/4$ and $N/2$. The distribution for honest nodes follows Eq. 1 and for dishonest nodes follows Eq. 2.

$$P(A) = \sum P(\{(e_1, ..., e_N)\}) = \binom{N}{k} \cdot p^k (1-p)^{N-k} \quad (1)$$

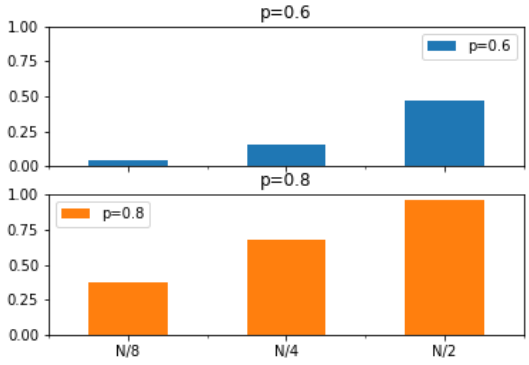
$$P(D) = \sum P(\{(e_1, ..., e_N)\}) = \binom{N}{k} \cdot q^k (1-q)^{N-k} \quad (2)$$

Analyzing Fig. 3, it can be seen that for $p = 0.6$, the probability of the rule being valid is negligible, and may be discarded, which can also be seen in Table I. As for $p = 0.8$, confirmations above $N/4$ prove to be sufficiently reliable, with a probability greater than fifty percent in all cases, which can be seen in Table II. It is interesting to note that with $p = 0.8$ the difference between the probabilities for $N/2$ and $N/4$ are very small, making $N/4$ an acceptable choice for ensuring network security.

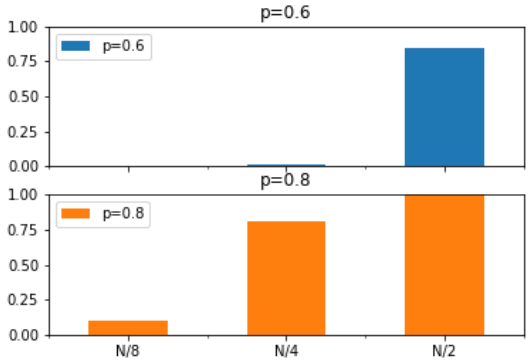
TABLE I: Results for $p = 0.6$

Nº of nodes (N)	Min. accepted (k)	Probab. of $A > k$
10	10/8	0.044
10	10/4	0.154
10	10/2	0.466
50	50/8	0
50	50/4	0.013
50	50/2	0.844
100	100/8	0
100	100/4	0.001
100	100/2	0.956

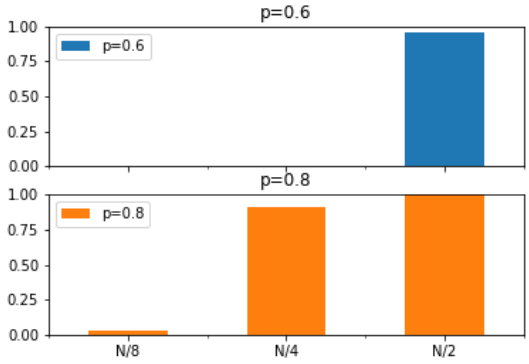
From the analysis presented, it is possible to conclude that $N/2$ is the ideal value to validate the rule. It is also possible to observe that for $p = 0.6$ having few nodes ($N = 10$), the values for confirmation are still no more than 0.5, which shows that to guarantee security in the network with few nodes it is necessary to wait for a little more than half of the nodes to approve the rule. For $p = 0.8$, high-reliability values start from $N/4$, regardless of the number of nodes, which can be advantageous if the node has a high degree of confidence in the other nodes in the network, which makes it interesting to increase the speed of updating the rules on your devices.



(a) $N = 10$



(b) $N = 50$



(c) $N = 100$

Fig. 3: Comparison of results of approval and rejection of rules when using 10, 50, and 100 nodes

TABLE II: Results for $p = 0.8$

Nº of nodes (N)	Min. accepted (k)	Probab. of $A > k$
10	10/8	0.375
10	10/4	0.677
10	10/2	0.960
50	50/8	0.103
50	50/4	0.813
50	50/2	0.999
100	100/8	0.025
100	10/4	0.912
100	10/2	0.999

VI. Conclusion and Future Works

The proposed solution is an evolution of a previous work in which a distributed architecture for intrusion detection in IoT networks using smart contracts in blockchain was developed. A statistical study was carried out to assess the minimum consensus required between nodes to ensure that security checks are legitimate. This study concluded that it is possible to accept the legitimacy of security checks, with a probability greater than fifty percent, waiting for at least half of the nodes to ensure their legitimacy. The study also demonstrated scenarios where the nodes have a high degree of trust with each other, in these scenarios a quarter of confirmations is sufficient to guarantee the legitimacy of security checks.

As future work we have:

- analysis of more complex scenarios with different minimum values of consensus and different probabilities of acceptance for transactions in the Binomial model;
- development of analytical models that consider network and time parameters, for example, using the *mainnet* of the Ethereum network and using a Poisson-based statistical model to assess the minimum time to reach consensus;
- competitive analysis between different smart contract platforms described by [32] to achieve greater speed and/or lower cost between transactions.

Acknowledgment

This work was supported in part by CNPq - Brazilian National Research Council, Grant 312180/2019-5 PQ-2, Grant BRICS 2017-591 LargEWiN, and Grant 465741/2014-2 INCT in Cybersecurity, in part by CAPES - Brazilian Higher Education Personnel Improvement Coordination, Grant 23038.007604/2014-69 FORTE, and Grant 88887.144009/2017-00 PROBRAL, in part by the Brazilian Ministry of the Economy, Grant 005/2016 DIPLA, and Grant 083/2016 ENAP, in part by the Institutional Security Office of the Presidency of Brazil, Grant ABIN 002/2017, in part by the Administrative Council for Economic Defense, Grant CADE 08700.000047/2019-14, and in part by the General Attorney of the Union, Grant AGU 697.935/2019.

References

[1] Gartner, Inc., *Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015*, Nov 2015. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2015-11-10-gartner-says-6-billion-connected-things-will-be-in-use-in-2016-up-3

[2] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and Other Botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[3] H. G. C. Ferreira and R. T. de Sousa Junior, "Security analysis of a proposed internet of things middleware," *Cluster Computing*, vol. 20, no. 1, pp. 651–660, 2017.

[4] A. A. Y. R. Fares, F. L. de Caldas Filho, W. F. Giozza, E. D. Canedo, F. L. L. de Mendonça, and G. D. A. Nze, "DoS Attack Prevention on IPS SDN Networks," in *2019 Workshop on Communication Networks and Power Systems (WCNPS)*. IEEE, 2019, pp. 1–7.

[5] B. V. Dutra, J. F. Alencastro, F. L. Caldas Filho, L. M. C. Martins, R. T. de Sousa Jr., and R. O. Albuquerque, "HIDS by signature for embedded devices in IoT networks," in *Actas de las V Jornadas Nacionales de Investigación en Ciberseguridad (JNIC 2019)*. Cáceres, Spain: Universidad de Extremadura, Jun 2019, pp. 53–61.

[6] D. G. V. Gonçalves, G. d. O. Kfouri, B. V. Dutra, J. F. d. Alencastro, F. L. d. Caldas Filho, L. M. C. e. Martins, R. d. O. Albuquerque, and R. T. de Sousa Jr, "IPS architecture for IoT networks overlaid on SDN [Arquitetura de IPS para redes IoT sobrepostas em SDN]," in *XIX Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, São Paulo-SP, 2019.

[7] G. O. Kfouri, D. G. V. Gonçalves, B. V. Dutra, J. F. d. Alencastro, F. L. Caldas Filho, L. M. C. Martins, B. J. G. Praciano, R. d. O. Albuquerque, and R. T. de Sousa Jr, "Design of a Distributed HIDS for IoT Backbone Components," in *FedCSIS (Communication Papers)*, Leipzig, Germany, 2019, pp. 81–88.

[8] R. Yuan, Y.-B. Xia, H.-B. Chen, B.-Y. Zang, and J. Xie, "ShadowEth: Private Smart Contract on Public Blockchain," in *J. Comput. Sci. Technol.*, vol. 33, 2018, pp. 542–556.

[9] F. Sabahi and A. Movaghar, "Intrusion detection: A survey," in *2008 Third International Conference on Systems and Networks Communications*, 2008, pp. 23–26.

[10] D. Wagner and P. Soto, "Mimicry attacks on host-based intrusion detection systems," in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, 2002, pp. 255–264.

[11] M. F. Elrawy, A. I. Awad, and H. Hamed, "Intrusion detection systems for IoT-based smart environments: a survey," *Journal of Cloud Computing*, vol. 7, no. 21, Dec 2018.

[12] S. Xie, Z. Zheng, W. Chen, J. Wu, H.-N. Dai, and M. Imran, "Blockchain for Cloud Exchange: A Survey," *Computers & Electrical Engineering*, vol. 81, p. 106526, Jan 2020.

[13] R. Agrawal, P. Verma, R. Sonanis, U. Goel, A. De, S. A. Kondaveeti, and S. Shekhar, "Continuous Security in IoT Using Blockchain," in *2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Calgary, AB, Canada, 2018, pp. 6423–6427.

[14] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," *2017 IEEE International Congress on Big Data (BigData Congress)*, pp. 557–564, 2017.

[15] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A Survey," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8076–8094, 2019.

[16] D. Carboni, "Feedback based reputation on top of the bitcoin blockchain," *ArXiv*, vol. abs/1502.01504, 2015.

[17] R. A. Bruce, R. T. de Sousa Júnior, F. L. L. de Mendonça, J. P. Pimentel, M. T. de Holanda, and F. L. de Caldas Filho, "Blockchain for Interbank Operations [Blockchain para Operações Interbancárias]," in *Atas das Conferências Ibero-Americanas WWW/Internet 2019 e Computação Aplicada 2019*, Lisbon, Portugal, 2019.

[18] C. Laneve, C. S. Coen, and A. Veschetti, *On the Prediction of Smart Contracts' Behaviours*. Cham, Switzerland: Springer International Publishing, 2019, pp. 397–415.

[19] M. Bartoletti, "Smart Contracts Contracts," *Frontiers in Blockchain*, vol. 3, p. 27, Jun 2020.

[20] V. Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform," Ethereum Foundation, Tech. Rep., 2015. [Online]. Available: https://ethereum.org/en/whitepaper/

[21] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, and J. Han, "When Intrusion Detection Meets Blockchain Technology: A Review," *IEEE Access*, vol. 6, pp. 10 179–10 188, 2018.

[22] S. Raza, L. Wallgren, and T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things," *Ad Hoc Networks*, vol. 11, no. 8, pp. 2661–2674, May 2013.

[23] S. Madhawa, P. Balakrishnan, and U. Arumugam, "Data driven intrusion detection system for software defined networking enabled industrial internet of things," *Journal of Intelligent & Fuzzy Systems*, vol. 34, pp. 1289–1300, 2018, 3. [Online]. Available: https://doi.org/10.3233/JIFS-169425

[24] H. Sedjelmaci, S. M. Senouci, and M. Al-Bahri, "A lightweight anomaly detection technique for low-resource IoT devices: A game-theoretic methodology," in *2016 IEEE International Conference on Communications (ICC)*, Kuala Lumpur, Malaysia, May 2016, pp. 1–6.

[25] A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman, and A. Alazab, "A Novel Ensemble of Hybrid Intrusion Detection System for Detecting Internet of Things Attacks," *Electronics*, vol. 8, no. 11, Oct 2019.

[26] A. A. Diro and N. Chilamkurti, "Distributed attack detection scheme using deep learning approach for Internet of Things," *Future Generation Computer Systems*, vol. 82, pp. 761–768, Aug 2018.

[27] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[28] B. B. Rad, M. Masrom, and S. Ibrahim, "Evolution of computer virus concealment and anti-virus techniques: A short survey," *CoRR*, vol. abs/1104.1070, 2011. [Online]. Available: http://arxiv.org/abs/1104.1070

[29] T. L. Sperling, F. L. Caldas Filho, R. T. de Sousa Jr., L. M. C. Martins, and R. L. Rocha, "Tracking intruders in IoT networks by means of DNS traffic analysis," in *2017 Workshop on Communication Networks and Power Systems (WCNPS)*. Brasília-DF: IEEE, 2017, pp. 1–4.

[30] T. L. Sperling, B. A. França, F. L. Caldas Filho, L. M. C. Martins, R. O. Albuquerque, and R. T. de Sousa Jr., "Evaluation of an IoT device designed for transparent traffic analysis," in *2018 Workshop on Communication Networks and Power Systems (WCNPS)*. Brasília-DF: IEEE, 2018, pp. 1–5.

[31] K. Bhargavan, C. Fournet, M. Kohlweiss, A. Pironti, P.-Y. Strub, and S. Zanella-Béguelin, "Proving the TLS Handshake Secure (As It Is)," in *Advances in Cryptology – CRYPTO 2014*, J. A. Garay and R. Gennaro, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 235–255.

[32] Z. Allam, "On Smart Contracts and Organisational Performance: A Review of Smart Contracts through the Blockchain Technology," *Review of Economic and Business Studies*, vol. 11, no. 2, pp. 137–156, 2019.