A Cryptographic Technique for Communication among IoT Devices using Tiger192 and Whirlpool

Bismark Tei Asare[1]
Lab-STICC, CNRS, UMRS 6285
Université De Bretagne Occidentale
F-29200 Brest, France
Cyber Security Division, CRITAC, Ghana
Directorate of Info. Assurance & Intelligence
CRITAC, Ghana

Kester Quist-Aphetsi[2]
Computer Science Department
Ghana Communication Technology University
Cyber Security Division, CRITAC, Ghana
Directorate of Info. Assurance & Intelligence
CRITAC, Ghana

Laurent Nana[3]
Lab-STICC, CNRS, UMRS 6285
Université De Bretagne Occidentale, F-29200 Brest, France

***Abstract*—The heterogeneous standards and operational platforms of IoT devices, introduce additional security loopholes into the network thereby increasing the attack surface for the IoT. Most of the devices used in these IoT systems are not secure by design. Such vulnerable devices pose a great threat to the IoT system. In recent times, there have been a lot of research works on improving existing mechanisms for securing IoT data at both the software and hardware levels. Although there exist cryptographic research solutions to secure data at the node level in IoT systems, there is not a lot of these security solutions that target securing both the IoT data and validating IoT nodes. The Authors propose a cryptographic solution that uses double hashing to provide improved security for IoT node data and validating nodes in IoT system. A cryptographic mechanism that is composed of the Tiger192 cryptographic hash and the whirlpool hash function is proposed in authenticating IoT data and validating devices in this paper. The use of digital ledger technology and cryptographic double hashing algorithm provided enhanced security, privacy, and integrity of data among IoT nodes. It also assured the availability of IoT data.**

***Keywords*—IoT devices; whirlpool; Tiger192; internet of things security; cryptographic communication**

I. Introduction

This paper extends an earlier conference paper submitted to the international Conference on Communications, Signal Processing and Networks / International Conference on Cyber Security and Internet-of-Things ICCSPN/ICSIoT. In our previous paper, we proposed and used a cryptographic primitive that involved the RC4 cryptographic algorithm and the whirlpool protocol in encrypting and validation of data within IoT systems [1]. The capacity of the internet of things to process large streams of data in real-time and its flexible adaptation for all environments makes it a widely adopted technology option for the collection, analysis and storage of critical data across many industrial fields as well as academia and Government installations. The spike in the adoption of the Internet of Things (IoT) across these various sectors makes it also a good target for cyber-attackers to exploit the vulnerabilities in the network. Internet-of-Things (IoT) can stream and support the creating of real time data to create new value propositions for small to large businesses, academia and governments. This unique quality of IoT system makes it one of the preferred technology of choice across all sectors of life [2]. The benefits of the innovation that IoT systems offer have been a good motivation for a lot more businesses, governments, and society to embrace in expanding access and increasing inclusiveness in the total monitoring, processing, storage, and communication of critical data in these sectors of life. The benefits that IoT systems offer have equally motivated and attracted the incidences of cyber-attacks on these systems towards the exploitation of the vulnerabilities in these connected systems.

Internet-of-Things involves several edge devices that connect to either a centralized node or distributed edge nodes to help aggregate critical data that is sensed from the immediate environments of these edge devices. The sensed data is therefore communicated through different communication protocols to the nodes. There exist several communication protocols that IoT devices adopt in transmitting data from one node to the other. These protocols include Bluetooth, WiFi, Satellite, Radio Frequency Identification (RFID), Near Field Communication (NFC). Most IoT systems use a combination of these communication protocols to connect and communicate data between each other because of the different connection requirements and capabilities from these edge devices of which sensors and actuators are the main actors in that category. These various communication protocols have their strengths as well as security vulnerabilities [3].

There are several cryptographic primitives that are used to provide privacy, integrity and confidentiality enhancements to data in IoT systems. These primitives have unique hardware as well as software platform requirements that need to be met in order to fully and effectively secure the data. Although some of these primitives have been around for decades, their ability to secure data is still relevant in recent times. The availability of modern hardware device with their heterogeneous design and

operational specifications has resulted in creating incompatibilities in the dependencies for platform execution that affect the latency and throughput of these cryptographic primitives. Some classical ciphers have been broken and that makes them weak and ineffective. Such ciphers intend introduce additional vulnerabilities to any network that adopt them to secure its data. This is because, these ciphers then serve as a weak link through which cyber-attacks could be launched on the network. Man-in-the-middle attacks and its associated threats have become common place in recent IoT cyber security incidence reports. At both the system and application levels, hacking activities have resulted in data corruption, illegal data transfer and in some cases destruction of critical hardware.

There have been recent developments of several cryptographic based solutions to address IoT device security challenges that satisfy the unique operational environments of the devices to support these devices to secure communication of sensed data even with obvious operational and environmental challenges of these devices including limited computational power and storage [4].

Several security interventions continue to be proposed to secure IoT systems. Although hash functions help in protecting the integrity of data, a weak hash function is equally as dangerous as not securing the data in the first place. There is therefore the need for a strong cipher that is energy efficient and yet effective to be deployed in maintaining the needed privacy, integrity and confidentiality to assure the security of data [5]. Most ciphers secure IoT systems with particular emphasis to either the software or application layer, whiles others target the hardware or the physical layer to ensure adequate security for IoT nodes are provided to complement firewall solutions.

Several security interventions continue to be proposed to secure IoT systems. Although hash functions help in protecting the integrity of data, a weak hash function is equally as dangerous as not securing data in the first place. There is therefore the need for a strong cipher that is energy efficient and yet strong or effective to be deployed in maintaining the needed privacy, integrity and confidentiality to assure the security of data [5]. Most ciphers secure IoT systems with particular emphasis to either the software or application layer, whiles others target the hardware or the physical layer to ensure adequate security for IoT nodes are provided to complement firewall solutions.

The use of a cryptographic solution that involves using hashing functions and digital signature scheme to provide security to node data as well as device validation is lacking in existing reviewed works.

The paper proposes a secure cryptographic solution that ensures non-repudiation of sending activities to help with device authentication, and message validation for constrained devices in IoT systems.

The cryptographic solution consisting of Tiger192, and whirlpool hashing algorithm provide message authentication and source data validation for the communicating nodes among IoT devices. The double hashing mechanism increases resistance to hash collisions of the cryptographic solution, thus used to increase the difficulty levels in guessing the content of the messages particularly brute force attacks and dictionary attacks. The Tiger192 cryptographic hash was used because it generates a shorter digest that maps to even longer messages.

The paper is organized into five sections. Section 2 describes background notions for the paper. The review of related works relevant to the paper is done in Section 2. Section 3 describes the methodology used in the paper. Section 4 discusses the results and section 5 concludes the paper and presents expected future work.

II. Related Work

A. Whirlpool Hash Function

The whirlpool function is composed of iteration of compression function with 512-bit key space to produce a 512-bit block dedicated cipher. To encrypt data of any size, the data is padded. It is adoptable to hardware implementations on both 8-bit and 64-bit platforms. It uses a substitution box where it generates randomly its 512-bit keys to provide digital signature to data [6].

B. The Tiger 192 Hash Function

This hash function uses large translation tables and runs well on 64-bit platforms to produce a much stronger 24 bytes long output hash. It includes an internal state size of 192 bits, and block size of 512 bit. The 192-bit key size provides a stronger and better encryption. It also supports the secure exchange of keys through the internet for encryption and authentication between two communicating parties.

The Tiger and its variant hash functions consumed less energy and yet provided an enhanced security among its peers. The cost in terms of energy consumption requirements for the Tiger192 is light weight as compared to other hash functions in its category, but it produces an efficient and effective hash value that is suitable for enhancing the security of data [7]. In [8], the Tiger hash was adopted to ensure the privacy and integrity of patients' critical health data. Machine learning techniques together with a Tiger hash based cryptographic protocol were implemented to secure the communication of critical medical data of patients across several mobile medical devices and systems. Secure cloud communication scheme was based on the Tiger hash cryptographic algorithm to support secure access of cloud data. The Tiger hash was adopted at the device or the physical layer level for cloud user enrolling phases for authenticating and granting the appropriate access rights to verified users to access cloud data or services [9].

C. Internet of Things Security

Most of the devices that are used in the IoT systems were not originally built for large scale and massive data streaming purposes, yet these devices end up being used in networks that stream massive data posing a lot of security risk onto these networks. The devices then become and create a weak security link where hackers compromise such systems using such weak links as point of entry. These devices with weak security qualities and requirements have contributed to the rising number in the man-in-the-middle and it related attacks suffered by IoT networks in recent times [1][10].

In [11] the authors underscored the need for an appropriate security intervention that is efficient and scalable to help address the unique security challenges of IoT systems that cut across privacy concerns, inadequate authentication and authorizations, insecure interface designs for web, mobile and cloud as well as the absence of a security encryption at the transport layer for communication of IoT data. These devices and system vulnerabilities in IoT makes it susceptible to mand-in-the-middle attacks and other associated security incidences.

The authors identified the various implementation environments for IoT and their unique security requirements for an appropriate implementation of these security schemes to enhance the security of IoT systems. Blockchain based cryptographic mechanism was proposed to help detect and validate devices to maintain data integrity within an IoT system [12].

Every IoT security solution must include an architecture that supports cryptographic protocols and algorithms for data verification to ensure integrity and secure management of all devices and objects connected to the IoT [13].

D. Cryptographic Communication

The authors in [14] used a privacy preserving cryptographic protocol in securing location-based information as well as user critical data communicated to the cloud. The Elliptic Curve cryptographic protocol was used in exchanging and establishing secure keys between the sensor nodes in the vehicles as well as the parking areas to ensure secure and effective parking of vehicles. Zero-knowledge prove system was used to ensure the privacy of communicated information between the gateways and the cloud as vehicles searched for vacant slots to park.

In [15], an inbuilt authentication IoT platform was adopted for inventory automation. The security framework in their platform used secure and energy efficient cipher to support authentication, integrity, and confidentiality of data.

In [16], a distributed authentication encryption mechanism that is lightweight and energy efficient as well as effective at providing security for IoT was adopted and used. This encryption technique offered secure authentication and access mechanism for the IoT network. The Cipher block Chaining-Message CCM algorithm was proposed and used to encrypt data for transmission. The algorithm allowed the receiver to create a token for each sender during transmission. These tokens had expiration time to be used to help check against impersonation attacks.

A 64-bit block cipher consisting of the Feistel and a constant substitution-permutation network to encrypt data was used by the authors in [17]. The algorithm adopted fever rounds of encryption making it lightweight for IoT devices and it provided a secure framework for the IoT network to achieve their targeted results.

In [18][19][20], the privacy of sensor data was preserved using blockchain and cryptographic schemes to guide the design approach of an IoT system. In their design approach, a blockchain concept was adopted in preserving the data through the generation, procession, and exchange of data across storage location. The use of blockchain was adopted in ensuring a tamperproof distributed and decentralized storage of sensor data for edge devices as hosting environment in IoT.

In [21][22][23], key pairs are used for the generation of the HMAC (Hash Message Authentication Code). HMAC assured message authentication as well as node validation for the sender node. The Tiger 192 hashing function served as the authentication function in providing integrity for IoT data from the source nodes to the receiver node.

III. METHODOLOGY

In Fig. 1, several edge devices are connected to a centralized node to coordinate device enrolment, authentication and authorization towards the communication of sensed data from the edge devices. The various edge devices are identified using their unique IP addresses. The centralized node helps with registering and authenticating all the edge nodes. These connected edge devices collect critical data from their environment and transmit it to the centralized node. The centralized node has enhanced computing power to process the transmitted data by intelligently measuring, analyzing and interpreting the sensed data from the edge devices.

The node serves as a hub for group enrollment of all sensors by adopting a common authentication mechanism to share a configuration for these sensors $(DN_1 - DN_\infty)$. The node coordinates and manages symmetric key certificate for encryption of data. The sensor and the node employed the same pre-shared encryption keys for secured communication between them.

At the application layer level on these nodes is implemented a blockchain-based digital ledger that records the unique attributes and data across all the connected nodes. All the edge nodes are cryptographically linked to store the updated state of all the validated data, distributed across the nodes.

Edge device enrolment onto the dedicated centralized node happens in two steps. The device gets registered on the centralized node using a key exchange protocol used to provide the needed credentials. The registration and certificate authorities are implemented on the centralized node to help coordinate device enrolment as well as authentication of edge devices. The enrollment and authentication occur through device provisioning. The just-in-time provisioning approach is adopted.

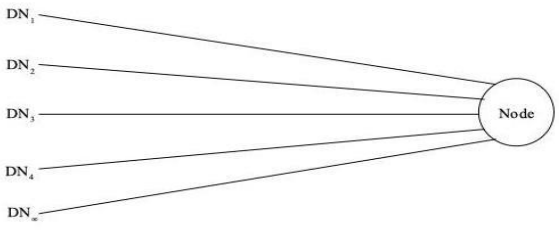

Fig. 1. Connected Edge Devices to a Node in an IoT System.

TABLE I. DIGITAL LEDGER IMPLEMENTATION TABLE AT THE NODE LEVEL

ID	SN	Data	Timestamp	Whirlpool	Tiger192
1	SN_1	D_1			
2					
3					
4					
5					
…	…	…	…	…	…
L	SN_L	D_L			

As shown in Table I, the distributed ledger to be implemented on the centralized nodes with its composition is displayed. It contains the various fields and components that constitute the digital ledger.

ID – Denotes the unique identifier to each connecting edge device or node in the IoT. It usually represents the component or part identification number of the sensor. For easy identification on a connected system, every object or connected device is assigned a unique sequence of hexadecimal values or alphanumeric value. The $ID_1 - ID_L$ denote the identifier of the first connected device to the last identifier respectively of the connected devices to the IoT. These identification labels are uniquely generated strings to represent each connected device[24].

SN – Represents the sensor or device name. IoT devices are named using various conventions and standardization criterion [25][26].

Data – This describes the message or information to be communicated. It is a plaintext data collected by an edge device or sensor from its immediate environment. It could be a temperature, hygrometer, electric voltage or other physical measurement value.

Timestamp – The timestamp component in the hash table denotes the specific date and time that the data or message arrived at the device. The timestamp consists of the date and time components that records the actual date and time the message or data arrived at the at the centralized node[27][28]. The date component comprises DD/MM/YYYY whereas the time component includes the HH:MIN:SEC. DD, MM, YYYY, HH, MIN, SEC represents Day, Month, Year, Hour, Minute, Seconds respectively.

Whirlpool – The message digest of the data to be communicated is produced using the whirlpool cryptographic hash function. The message digest is then stored in the whirlpool field, for each data.

Tiger192 – The digital fingerprint value or digital signature of the encrypted message is created using the Tiger192 cryptographic hash for each message. The digital fingerprint for message digest is stored in the Tiger192 field.

The whirlpool hash is computed using:

Hash (Data, Device Name, Timestamp, Previous Hash)

The plaintext message to be hashed is segmented into blocks.

$m_1, m_2, m_3, \dots, m_t$

H_o=initial value

$H_i = E(H_{i-1}, m_i) \oplus H_{i-1} \oplus m_i$intermediate hash value

H_t=Hash code value

m_i represents the current message block for the plaintext

E represents the block-cipher-based hash function for Whirlpool

H_i represents the intermediate hash value

H_{i-1}represents the hash value for the previous iteration.

H_t denotes the hash code value

The output hash value (H_i) is computed using the bitwise XOR operation on the current message block, the intermediate hash value from the previous iteration and the output of block-cipher-based hash function of Whirlpool (W).

The output hash code for the whirlpool cryptographic algorithm is a 512-bit size message digest [29].

The Tiger hashing algorithm is used to implement a Hash Message Authentication Code (HMAC).

Three main components constituted the Tiger 192 hashing algorithm. Key generation algorithm, Signing Algorithm, Verifying Algorithm [30].

The key generation phase:

The key generator ensures the generation of the private and public keys for the two nodes.

The private key of the sender node is used to generate the digital signature for the message using the resultant hash code value of the whirlpool hash and the sender private key as the input strings.

$Sig_1 = H(H_t, SP_rK)$

Where:

Sig_1 -- represents the digital signature generated at the message originating node.

H -- is the Tiger192 Hashing Algorithm.

H_t -- denotes the hash value code, a resultant message digest.

SP_rK -- represents the sender's private key.

Sig_1 is the digital signature or the Hash Message Authentication Code (HMAC) for the message digest from the node originating the data to be communicated. The message to be sent to the receiver is a composition of the sig_1 and H_t.

At the receiver node,

The Private key of the receiver node (RP_rK) is used to decrypt the signature.

$Sig_2 = H(H_t, RP_rK)$

Where:

Sig_2 -- represents the digital signature generated at the receiver node.

H -- is the Tiger192 Hashing Algorithm.

H_t -- denotes the hash value code, a resultant message digest.

RP_rK -- represents the receiver's private key.

The resultant hash from the decryption is compared with the hash of the message.

A. Signature Verification Process

The signature verification process is performed using the private key of the receiver node, the hash value (H_t) and the signing algorithm in Tiger192. It is carried out at the base station serving at the sink nodes (T_1 and T_2) using the sig_1 and sig_2 values.

1) Obtain hash code value H(M) and sig_1 (HMAC) from source node.

2) Apply private key of receiver node on the hash code to obtain sig_2 (HMAC).

3) Compare the sig_1 and sig_2. HMAC and HMAC values for source and receiver nodes respectively.

4) Check for same. strings in the sig1 and sig2. If fails, reject signature and message.

5) Otherwise, use the reverse whirlpool on the hash to regenerate the message.

IV. Result

As shown in Fig. 2, nodes T_1 *and* T_2 are IoT nodes that have adequate computational and storage capacity to support the provision of connectivity for edge devices mainly sensors.

Both nodes adopted a centralized approach towards device enrollment and authentication for the IoT device provisioning. Registration and Certificate authorization mechanisms were implemented on these nodes (T_1 *and* T_2) to help them manage, coordinate and control the smooth enrollment and management of all the edge devices that were connected to them. The node serves as a hub for group enrollment of all sensors by adopting a common authentication mechanism to share a configuration for these sensors ($DN_1 - DN_\infty$). The node coordinates and manages symmetric key certificate for encryption of data. The sensor and the node employ the same pre-shared encryption keys for secured communication between them.

Sensor data from the edge devices are hashed using the whirlpool cryptographic hash function. The encrypted data is stored on the centralized node on each of the two nodes (T_1 *and* T_2). The stored encrypted data is stored in a blockchain-based digital ledger. The distributed ledger technology implemented on the two connected nodes ensured the replication of storage of encrypted data across the two connected nodes. The use of the digital ledger and the subsequent duplication across the connected nodes eliminate the occurrences of single point of failure that would result in data loss in the IoT.

Table II represents data storage of hashes in the digital ledger and the duplication of storage on the blockchain digital ledger across the connected sink nodes.

The system in Fig. 2 demonstrated a digital ledger containing encrypted data which is based on the blockchain digital signature concepts. The hash table with their content is shared across the two connected nodes; thus, a source node and a destination node.

TABLE II. Displayed Result

ID	SN	Data	Timestamp	Whirlpool	Tiger192
1	2	546541	06/05/2019 01:04	837b2f65671b3f0ce5ace81f3fa251ea7a2c5c5fcba211c234f2a23f83654ea406ecd28f90d6e7569b1ffc94732ca6d977ffe3cda0ec8b44d1619cf8bae22bcf	372049593394e34bbe0cdeb5aafd04c1e8d1c89377839723
2	3	669566	06/05/2019 07:56	f045dfeab2c2ba445dbf95ebfa9dbbcbdc204f40094b88221ed8873657e3fbe5986afa6eb522873614947452c1c44587193ba5d2d7ae858bb39102f23e7195da	0245b4eb07777000a4cef45323f96c663566e67d7515b553
3	4	659526	06/05/2019 04:38	367d7dbea6ed284bb82802c6ffca36921225f7e39ebfdbd3516d94ab828b4cfed19a08c5840666982c5a21a26cdb98aa333693240da63f58eb6795a6d9e40508	aa2dc714983dad807cabb5432a164de4541f3a11f044fb42
4	1	454986	06/05/2019 11:27	636a0c83e50f159b0b5bfebdce07c1f8a67b9320508bbedcbfff3b5963c9c35f7f3745109f0cc9d3b91b50099173556d56dbb06f5771f8c6f6ed109b228d32fd	cb3ebced2ed66321a21be77063bd4f7ea355188a5eeaf14f
5	2	365495	06/05/2019 06:05	121d28efb1649a007a5307c314a88c5f48c95405e59c6252a1adf18a8a3cda32cf2d32c76be51dd9d7cd197091c58134706983140ce9bb8a9f24a0866ebb480d	1be15d54f30f24d7c7f6a1cd757e39c6e40f5e53080f098b

Fig. 2. Two Nodes T1 and T2.

The hash function ensured that the data and the unique components of the hash function were not tampered with, since any alteration of any of the hashing components will result in a different hash. The distributed storage of the digital ledger between the source and the destination nodes is compared for detection of tampering of IoT messages. The hash tables of both nodes must produce same values. Any modification of the message will produce a different output for the hash table. The use of the cryptographic algorithm and the hash function guaranteed the security, privacy, confidentiality, and availability of the IoT data. The Tiger192 cryptographic hash generated a digital signature for each content of the message. The private key of the sending device is used in generating the digital signature of the content of the message. The digital signature produces a shorter message digest that maps onto the content of messages. The Tiger 192 generated a digital signature for each cryptographic encryption produced. The digital signature assists in authentication of the content of messages. The Tiger 192 signed messages provided non-repudiation in validating the authenticity of the sending node. The public key of the sending node can be publicly verified even by unintended recipients within the network. The digital signature is based on the content of the message being signed. Both the ciphertext and digital signature are communicated between the communicating nodes.

Message integrity and authenticity is verified using the HMAC (keyed-hash message authentication code). The shared secret between the communicating nodes (T_1 and T_2) provided data origin authentication as well as message integrity.

V. Conclusion and Future Work

This paper adopted a hybrid cryptographic scheme that included the Tiger192 cryptographic algorithm and the whirlpool hash function to support secure communication of IoT devices. Data to be communicated was hashed using the whirlpool cryptographic hashing function. The Tiger 192 hashing function was used to generate a digital signature, a shorter digest that tagged and mapped onto the content of messages. The whirlpool hash served as the building block for encrypted message and the message authentication code or digital signature is then communicated between the source node and the destination node. The security and strength of a cryptosystem is based on the length of the key size. The 192-bits key size assured a stronger and produced a shorter mapped digest for all messages particularly for longer messages. The use of the Tiger cryptographic algorithm provided a complementary security layer to assure message authentication using the HMAC. Tampering of data incidences are detected and addressed since the digital ledger replicates storage of encrypted data across all connected nodes. The storage of data across the connected sink nodes assured data availability since single point of failure incidences were eliminated with the digital ledger technology. Node authentication assuring the identity of the source of the data is enforced using the key public key of the sender node to enforce non-repudiation. It also protected the integrity of data by validating the genuineness of the data communicated using integrity authentication through the comparing of the digital signature tags on the sender and receiver nodes. The double hashing used increased the resistance to hash collisions of the cryptographic solution, thus used to increase the difficulty levels in guessing the content of the messages particularly brute force attacks and dictionary attacks. The double hashing cryptographic mechanism consisting of the Tiger192 cryptographic hashing scheme, and the whirlpool hash function increased the security, privacy, and integrity of IoT data. The use of the digital ledger technology assured availability of data.

The use of the digital signature assisted in authenticating IoT data whereas the validating devices in this paper. The use of digital ledger technology and cryptographic scheme of double hashing algorithm provided enhanced security, privacy, and integrity of data among IoT nodes. It also assured the availability of IoT data.

The key pairs used for the generation of the HMAC assured message authentication as well as node validation for the sender node. The public key of the sender node helped in enforcing non-repudiation of the origin of data as well as device verification. The authentication function provided by the Tiger 192 provided integrity for data from the source nodes to the receiver node. Since the public key of the sending device is available within the network, the source of the message can be validated enforcing non-repudiation.

An implementation of this combined cryptographic algorithm on an IoT platform would be explored for future works.

References

[1] B.T. Asare, K. Quist-Aphetsi, L. Nana, “Using RC4 and whirlpool for the encryption and validation of data in IoT,” Proceedings - 2019 International Conference on Cyber Security and Internet of Things, ICSIoT 2019, 114–117, 2019, doi:10.1109/ICSIoT47925.2019.00027.

[2] G. Strategy, L. Council, “Internet of Things : Where Your Competitors Are Investing Overview,” Gartner, 2020.

[3] S. Hashemi, M. Zarei, “Internet of Things backdoors: Resource management issues, security challenges, and detection methods,” Transactions on Emerging Telecommunications Technologies, (August), 1–25, 2020, doi:10.1002/ett.4142.

[4] D. Di Luccio, S. Kosta, A. Castiglione, A. Maratea, R. Montella, “Vessel to shore data movement through the Internet of Floating Things: A microservice platform at the edge,” Concurrency Computation , (March), 1–13, 2020, doi:10.1002/cpe.5988.

[5] K. Christidis, M. Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things,” IEEE Access, 4, 2292–2303, 2016, doi:10.1109/ACCESS.2016.2566339.

[6] P.S.L.M. Barreto, V. Rijmen, The WHIRLPOOL Hashing Function, 1384--1385, 2011.

[7] R. Damasevicius, G. Ziberkas, V. Stuikys, J. Toldinas, “Energy consumption of hash functions,” Elektronika Ir Elektrotechnika, 2012, doi:10.5755/j01.eee.18.10.3069.

[8] R. Venkatesan, B. Srinivasan, P. Rajendiran, “Tiger hash based AdaBoost machine learning classifier for secured multicasting in mobile healthcare system,” Cluster Computing, 2019, doi:10.1007/s10586-018-2241-9.

[9] K.M. Prabha, P. Vidhya Saraswathi, “Tiger hash kerberos biometric blowfish user authentication for secured data access in cloud,” in Proceedings of the International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), I-SMAC 2018, 2019, doi:10.1109/I-SMAC.2018.8653713.

[10] C. Kolias, G. Kambourakis, A. Stavrou, J. Voas, “DDoS in the IoT: Mirai and other botnets,” Computer, 50(7), 80–84, 2017, doi:10.1109/MC.2017.201.

[11] E. Bertino, N. Islam, “Botnets and Internet of Things Security,” Computer, 2017, doi:10.1109/MC.2017.62.

[12] M. Banerjee, J. Lee, K.K.R. Choo, "A blockchain future for internet of things security: a position paper," Digital Communications and Networks, 2018, doi:10.1016/j.dcan.2017.10.006.

[13] A.R. Sadeghi, C. Wachsmann, M. Waidner, "Security and privacy challenges in industrial Internet of Things," in Proceedings - Design Automation Conference, 2015, doi:10.1145/2744769.2747942.

[14] I. Chatzigiannakis, A. Vitaletti, A. Pyrgelis, "A privacy-preserving smart parking system using an IoT elliptic curve based security platform," Computer Communications, 89–90, 165–177, 2016, doi:10.1016/j.comcom.2016.03.014.

[15] I. Batra, S. Verma, Kavita, M. Alazab, "A lightweight IoT-based security framework for inventory automation using wireless sensor network," International Journal of Communication Systems, 33(4), 1–16, 2020, doi:10.1002/dac.4228.

[16] P. Sudhakaran, C. Malathy, "Energy efficient distributed lightweight authentication and encryption technique for IoT security," International Journal of Communication Systems, (August), 1–10, 2019, doi:10.1002/dac.4198.

[17] M. Usman, I. Ahmed, M. Imran, S. Khan, U. Ali, "SIT: A Lightweight Encryption Algorithm for Secure Internet of Things," International Journal of Advanced Computer Science and Applications, 8(1), 1–10, 2017, doi:10.14569/ijacsa.2017.080151.

[18] M. Chanson, A. Bogner, D. Bilgeri, E. Fleisch, F. Wortmann, "Blockchain for the IoT: Privacy-preserving protection of sensor data," Journal of the Association for Information Systems, 20(9), 1271–1307, 2019, doi:10.17705/1jais.00567.

[19] M. Samaniego, R. Deters, "Blockchain as a Service for IoT," Proceedings - 2016 IEEE International Conference on Internet of Things; IEEE Green Computing and Communications; IEEE Cyber, Physical, and Social Computing; IEEE Smart Data, IThings-GreenCom-CPSCom-Smart Data 2016, 433–436, 2017, doi:10.1109/iThings-GreenCom-CPSCom-SmartData.2016.102.

[20] M. Chanson, A. Bogner, D. Bilgeri, E. Fleisch, F. Wortmann, "Privacy-Preserving Data Certification in the Internet of Things: Leveraging Blockchain Technology to Protect Sensor Data," Journal of the Association for Information Systems, (March), 2019.

[21] M. Tuba, N. Stanarevic, "Relation between successfulness of birthday attack on digital signature and hash function irregularity," WSEAS Transactions on Information Science and Applications, 7(2), 186–195, 2010.

[22] B. Applebaum, N. Haramaty-Krasne, Y. Ishai, E. Kushilevitz, V. Vaikuntanathan, "Low-complexity cryptographic hash functions," Leibniz International Proceedings in Informatics, LIPIcs, 67(7), 1–7, 2017, doi:10.4230/LIPIcs.ITCS.2017.7.

[23] V.E. Balas, Intelligent Systems Reference Library 165 A Handbook of Internet of Things in Biomedical and Cyber Physical System, Springer, 2019.

[24] H. Aftab, K. Gilani, J.E. Lee, L. Nkenyereye, S.M. Jeong, J.S. Song, "Analysis of identifiers in IoT platforms," Digital Communications and Networks, 6(3), 333–340, 2020, doi:10.1016/j.dcan.2019.05.003.

[25] Y. Li, C. Network, N.D. Networking, R. Jian, "Naming in the Internet of Things," 1–7, 2014.

[26] Y. Jung, M. Peradilla, A. Saini, "Software-defined Naming, Discovery and Session Control for IoT Devices and Smart Phones in the Constraint Networks," Procedia Computer Science, 110, 290–296, 2017, doi:10.1016/j.procs.2017.06.097.

[27] P. Oser, F. Kargl, S. Lüders, "Identifying devices of the internet of things using machine learning on clock characteristics," Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 11342 LNCS, 417–427, 2018, doi:10.1007/978-3-030-05345-1_36.

[28] M. Shahid, G. Blanc, Z. Zhang, H. Debar, M. Shahid, G. Blanc, Z. Zhang, H. Debar, I. Devices, R. Through, M.R. Shahid, G. Blanc, Z. Zhang, "IoT Devices Recognition Through Network Traffic Analysis To cite this version : HAL Id : hal-01994156 IoT Devices Recognition Through Network Traffic Analysis," 2019.

[29] W. Stallings, "The whirlpool secure hash function," Cryptologia, 30(1), 55–67, 2006, doi:10.1080/01611190500380090.

[30] V. Rao, K. V. Prema, "Light-weight hashing method for user authentication in Internet-of-Things," Ad Hoc Networks, 89, 97–106, 2019, doi:10.1016/j.adhoc.2019.03.003.