SECURE AND PRIVACY-AWARE DATA COLLECTION ARCHITECTURE APPROACH IN FOG NODE BASED DISTRIBUTED IOT ENVIRONMENT

Moussa WITTI and Prof. Dimitri KONSTANTAS

Information Science Institute University of Geneva
Route de Drize 7, 1227 Carouge, Switzerland

ABSTRACT

In the era of Internet of Things, data are collected from heterogeneous wireless protocols such as ZigBee, WiFi, RFID, Bluetooth, sub-GHz, Z-Wave, 2G / 3G / 4G form smart sensors to fog and cloud platform. However, the collected data may contains sensitive information, which the owner does not want to be disclosure. Because of IOT architecture based on heterogeneous technologies, ensuring privacy and maintaining security are difficult. How to protect data and preserve privacy over network during end-to- end or hop-to-hop communication? In this paper, we propose an architecture approach for secure and privacy-aware data collection in Fog Node Based Distributed IOT environment.

KEYWORDS

Internet of Thing, privacy, security, data collection, fog

1. INTRODUCTION

The growth of smart devices communicated together or via a distributed platform has enabled data collection from sensors to fog/cloud in IOT environment. Each sensor is able to transmit collected data to a fog server. A multiple fog server sends all collect data to a cloud server, which performs data processing, analysis and monitoring. Data are transported thought a heterogeneous environment, stored, analysed and sometimes transformed during processing.

According to Gartner, by 2025, over 1 trillion smart sensors will be used around the world and more than half of these devices will concern latency sensitive applications [2][3] such as healthcare and smart city applications. Since fog computing has emerged to support latency sensitive applications interacting with edge and cloud platform. How should privacy be preserved, and how should security be ensured, while collecting data across the edge-fog-cloud environment? How should data be secured through life-cycle processes across the edge-fog-cloud? Furthermore, how should privacy-aware data collection be provided in a well-secured Fog Node-Based Distributed IOT environment?

In this paper, we aim to apply privacy and security requirements on some data identified and categorized as sensitive. Thus, we propose an architectural approach to secure and preserve privacy while data collection in IOT fog and cloud environment. The paper is structured as follows: after background and related work in Section 2, Section 3 focuses on privacy and security requirements in IOT-enabled platform, Section 4 presents our proposed approach,

Natarajan Meghanathan et al. (Eds) : CSEIT, CMLA, NeTCOM, CIoT, SPM, NCS, WiMoNe, Graph-hoc - 2019
pp. 19-32, 2019. © CS & IT-CSCP 2019 DOI: 10.5121/csit.2019.91302

Section 6 propose solution architecture, comparison analysis and Section 7 provides conclusions and gives direction for future work.

2. RELATED WORK AND BACKGROUND

Privacy and security issues are challenged and several security models for IoT have been designed. The rapid growth of IoT has extended Internet to any small smart devices in distributed environment [6] therefore has introduced a problem. As IoT environment is more heterogeneous, more complex [3] and maintaining security is very critical in distributed system as well as cloud and fog environment [4] [11] . Most research studies [6] [10] [19] [20] [21] [30] are focused on how to integrate security among application, perception and transport layers level for distributed or cloud environment such as IaaS (Infrastructure as a Service), SaaS (Software as Service), and PaaS (Platform as Service). To protect sensitive data a huge of privacy-preserving algorithms have been developed such as k-anonymity, l-diversity. The concept of k-anonymity has been introduced by L. Sweeney and P. Samarati [24] in order to preserve privacy. While l-diversity is a data anonymization technique based on generalization and suppression often with a loss of the quality of the information. L-diversity is defined as extension of the k-anonymity [15]. Another algorithm ‘t-closeness’ [21] has been developed to anonymize data [15] [25] This technique is an extension of l-diversity and designed to preserve the confidentiality of sensitive data while reducing the granularity of data representation.

Several framework has been designed to maintain security along to end-to-end communication in IoT-based solu-tions. Cisco has proposed IoT/M2M Security Framework to protect data confidentiality and provide role-based security mechanisms. Other such as Icon Labs’ Floodgate Security Framework provides cyber security standards for Industrial Automation and management Systems (IACS) according to ISA/IEC 6244 standard.

2.1 Privacy and confidentiality

There is no universal definition of privacy because it differs according to the economic, societal, religious and cultural characteristics of a given population [8]. This means that privacy depends on our preferences what we want to share as information without disclosing personal matters. Many factors affect what people consider private. Many factors influence what a person may consider private. It depends mainly on the culture and the societal context. It also depends on a given situation according to which the same information considered as private differently [13]. Other researchers like American law professor Alan Westin have defined three levels of privacy norms: political, socio-cultural and personal level [19] [23]. Other searcher as Daniel Solove has tried to classify the elements of privacy [26] according to six categories such as:

- the right to be left alone,
- a secret access
- the control of personal information
- identity of the person
- Privacy.

2.2. Privacy policy and law regulations

Privacy rules implementation dependent on the context of the society and country laws:

- European Union has implemented General Data Protection Regulation and Data Protection Directive to protect privacy. The article 8 of European Convention on Human Rights (ECHR) protect the individual and family right and privacy.

- United States have adopted three main federal laws which are Children's Online Privacy Protection Act (COPPA) to protected children under 13 age, Gramm-Leach-Bliley Act for privacy in financial institutions, Health Insurance Portability and Accountability Act for insurance companies use.

- Canada federal government provide Personal Information Protection and Electronic Documents Act (PIPEDA) to preserve privacy in data collection and electronic exchange.

- India government adopted by the end of 2000, The Information Technology Act 2000 improved in 2008 and in 2011 to integrate security practices and procedures to protect personal data or sensitive information.

2.3. Privacy concerns in Data Collection

Nowadays, a huge amount of data is collected from smart sensors and sent to fog and cloud processing system. IOT-enabled platforms must implement security and data protection rules following existing laws and regulations. The principle of privacy must be guaranteed. Sensitive data must be protected from attack and unauthorized access.

Because of the use of the Internet, IOTs inherit the same vulnerabilities as any computer device. How to preserve privacy and ensure security. Indeed IOTs are all potential victims of cyberattacks. An attack on a connected object can cause considerable damage to an IoT-enabled fog and cloud computing platform. From one point after a connection to a device communicating with the others, it possible to an attacker to can access the entire IoT-enabled platform. This creates a serious vulnerability and any confidential information on the network can be viewed from any connected device.

2.4. IOT main threats

Any IOT-enabled platform may experience the following types of attacks such as:

- DDOS (Distributed Denial of Service): massive attack on a network or a connected object in order to cause unavailability of the service or the server.
- Thingbot: multiple attacks from a network of large-scale cyber-attacks to take remote control of a connected object and spread malicious programs or access confidential data on an IOT platform.
- Man-in-the-Middle: interception of messages between two users by a malicious cyber-attacker with modification of the original message. Many MIM attacks on the IOT platform have been reported in smart Home and in the automotive era with connected object.

3. PRIVACY AND SECURITY REQUIREMENT IN IOT-ENABLED PLATFORM

Due to IOT architecture and its ubiquitous Internet connection [4], [12], [27], [32] maintaining security in IOT platform becomes more difficult.

3.1. IOT platform security requirements

Security requirements in IOT based architecture should be implemented along multi-layers [3][30]:

- Securing the perception layer:
- Securing the transport channel at the network layer using Transport Layer Security

(TLS), which is an encryption protocol to protect messages on the network, and provide secure channel to ensure privacy and data security.

- Securing data, files systems, and business applications at application layer

Yang et al. [30] has proposed a set of trust enhancing in IOT platform based on Key Exchange Management. Others as Bawany et al [3] have proposed an IOT security framework to prevent DDOS.

Thus, according to Yang et al. [30] and Bawany et al [3], an IOT-enabled platform should implement:

- IAM (Identity and Access Management),
- AAA (Authentication Authorization Accounting),
- K.E.M (Key Exchange and Management) for trust, and data integrity, confidentiality, availability, cryptography,
- I.A.A (Identification Authentication and Authorization)
- Devices resilience
- Trust: smart device trust and data trust
- Privacy: Data privacy, anonymity, unlinkability, unobservability, pseudonomity
- Network Security: TSL protocol
- Privacy-preserving policies: Data storage policy, location privacy, identity privacy, data processing and analytics privacy

Identity and Access Management (IAM) refers to users/groups identification and access to resources or applications. IoT-enabled platform IAM policies should implement identification mechanisms and role for users/groups to access a specified resource. Users belong to a group or multiple group with different roles. Multiple users may have the same role or privilege to access multiple resources.

IAM process is based on Authentication, Authorization, and Accounting (AAA) mechanism:

- User authentication refers to the process used to verify user’s claims through login/password or smart card access, secret code, fingerprint scan, secure ID generated automatically by a program or smart key, etc.

- User authorization is mechanism performed to verify the user’s access to resources or applications based on user’s group, user’s role or privileges.

- Accounting refers to the logging of the user's Authentication and Authorization mechanisms

Trust process in an IoT-enabled platform may be applied into data and devices level:

- Device trust refers to all mechanisms used to identify and recognize a component as trust and secure to communicate with other applications

- Data Trust defines the entire process to ensure that the data has never been altered during transport on the network. Data should be identical from the origin

Network security is built around three main objectives that are:

- Data Confidentiality: protecting data from unauthorized users
- Data integrity: ensuring data reliable and identical as from the origin

- Data availability: ensuring data available on the network for the right users when it is requested

3.2. Data security

We have organized data security approaches into four categories (see figure 1):

- Integrity and confidentiality of sensitive data to prevent the risk of tampering or injection or falsification
- Authenticity: data received must be authentic at the origin
- Non-repudiation: transmitted data should not be unknown to the sender
- Availability: ensure data availability reliably.

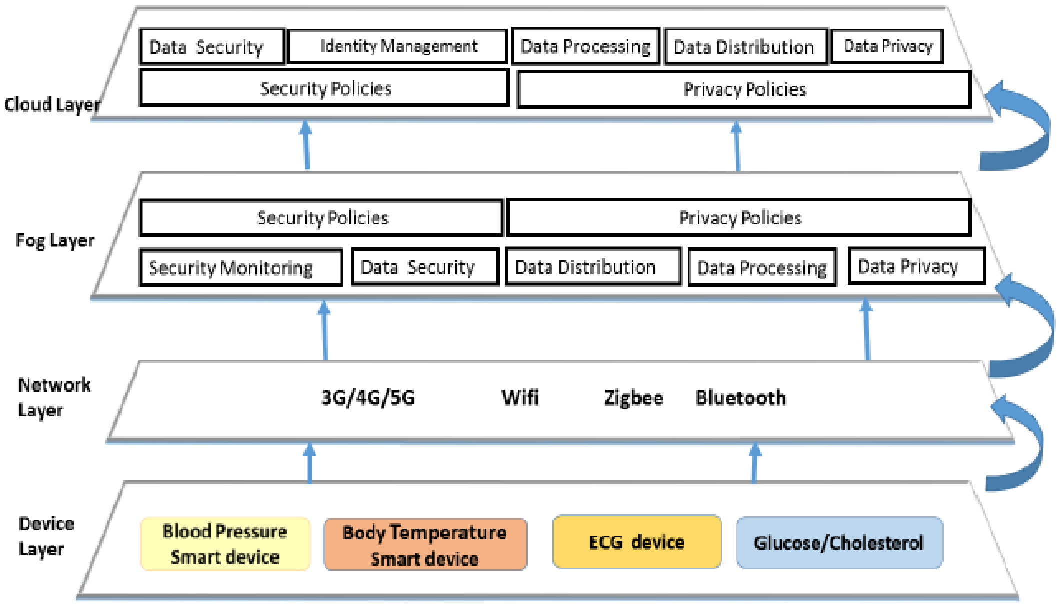


Figure 1: Data security and privacy management through IoT Layers

3.3. Data privacy

We have organized the privacy-preserving approaches into five categories (see figure 1):

- Privacy by cryptography
- Privacy by pseudonymization
- Privacy by anonymization
- Privacy by unlinkability,
- Privacy by unobservability

4. Proposed Approach

Data exchange in an IOT fog cloud environment may be secured in multiple manners and here we propose a bottom-up approach. We propose an architectural approach based on:

1- IOT devices identification/authentication/authorization process
2- Gateway and Wireless/Bluetooth access point control
3- Data protection while collecting using dynamic key and hash function on fog and cloud IOT environment

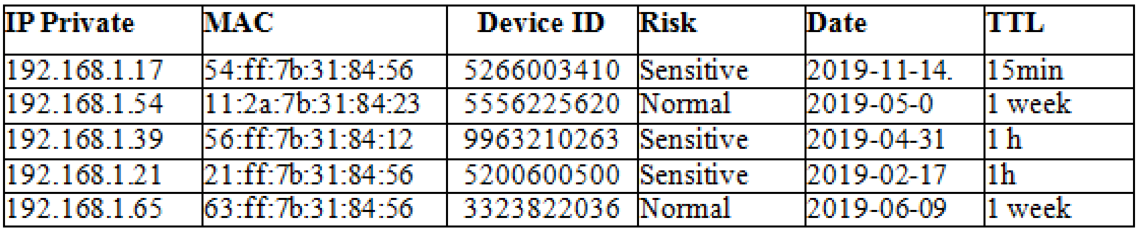
4.1. Device security

Most IOT devices in communication may be identified by an IP or media access control (MAC) address or by International Mobile Device Identity (IMEI). On the network, a malicious attacker can impersonate the IP address or MAC address to alter conveyed data or access to other resources.

In our approach, we propose life cycle Identity and Access Management (IAM) system in which each device must be identified by an ID on fog Nodes. A well-integrated IOT device security strategy must implement:

- Device identification system: in addition of IP and MAC address, any device must be authenticated by a specified ID with a role on the network
- Device identity lifecycle management system: device ID must change by the time to avoid spoofing in case of malicious attack. We define TTL - time to live.
- Device authentication and access control according security level and companies policies

Table 1. IOT devices security management.



IP Private	MAC	Device ID	Risk	Date	TTL
192.168.1.17	54:ff:7b:31:84:56	5266003410	Sensitive	2019-11-14.	15min
192.168.1.54	11:2a:7b:31:84:23	5556225620	Normal	2019-05-0	1 week
192.168.1.39	56:ff:7b:31:84:12	9963210263	Sensitive	2019-04-31	1 h
192.168.1.21	21:ff:7b:31:84:56	5200600500	Sensitive	2019-02-17	1h
192.168.1.65	63:ff:7b:31:84:56	3323822036	Normal	2019-06-09	1 week

4.2. IOT Access Point Control

Access point must be controlled according to the resource sensitivity. As devices are categorized according to data sensitivity, each devices has grant to a specified gateway to transmit data on the network. We propose a dynamic access control approach based on sensitive or non-sensitive data and associated risks. Only IOT device with a minimum of privileges can access to a control point or gateway.

4.3. Shared key online construction

In our approach, we propose to build a shared key online from conveyed data’s elements such as token ID, user ID, data correlation ID (cf. table 1). All such elements will be placed in a matrix according to a specified order known both by client/server side. Thus, the secret key generation process will be reinforced.

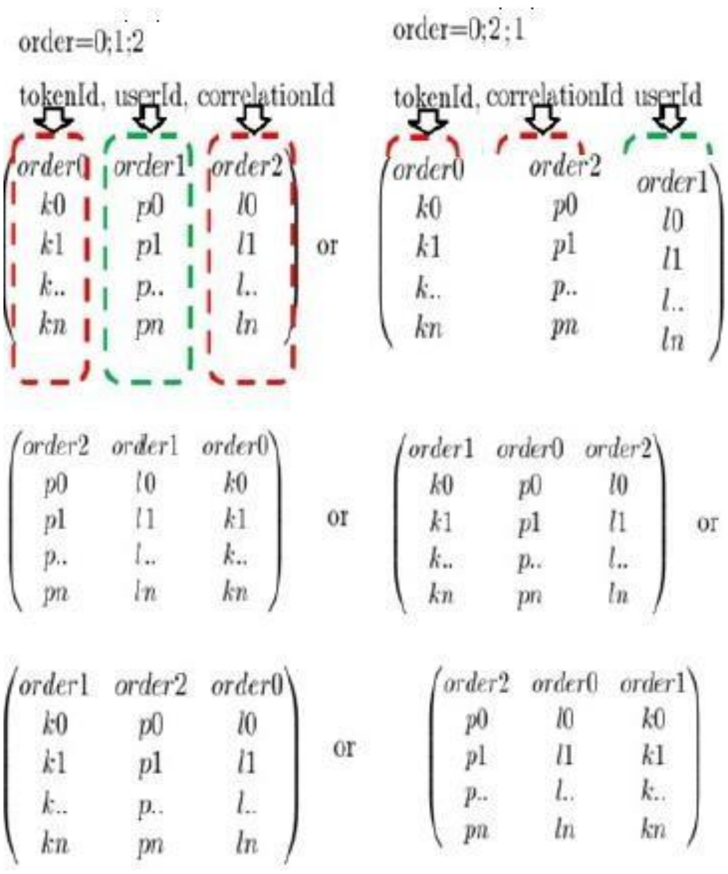


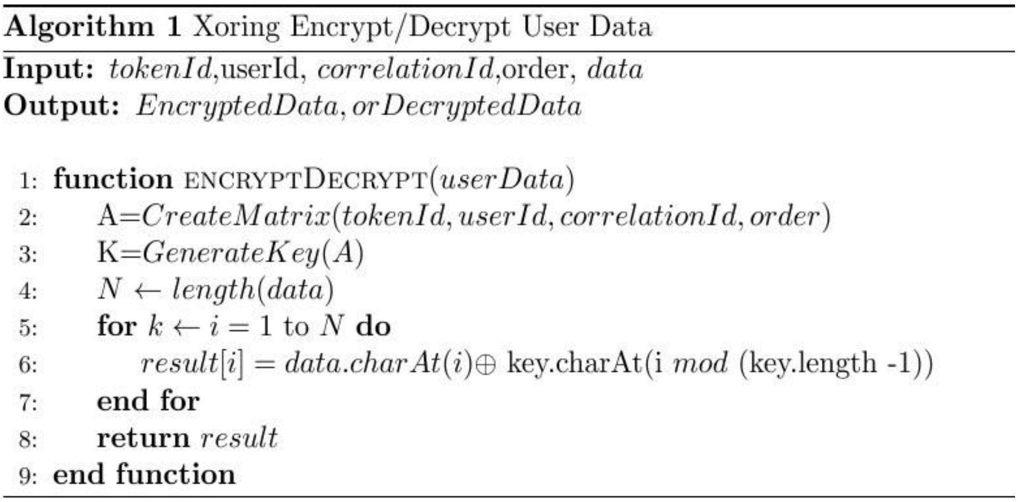
Figure 2: Secret Key Matrix Generation

The shared key is built online without complex calculations, which will not affect performance. The server knowns all dealers identified by their ID. Collected data are identified by correlation ID on the server side in the cloud during processing analytic stage.

For each request, a new token Id I generated. The user ID is related to the dealer while correlation ID is depending on data collection program.

4.4. Data encryption/decryption

To ensure privacy, data should be encrypted before transmitting on the network. Dealers may use shared key to encrypt/decrypt data. We propose XOR operation to compute efficiently with all dealers. The proposed algorithm generate the shared key based on shared key generation which is based on Token ID, User ID and Correlation ID placed in different rank according to a specified order kown by the server and dealers (cf. figure 2).



Algorithm 1 Xoring Encrypt/Decrypt User Data

Input: *tokenId*,userId, *correlationId*,order, *data*

Output: *EncryptedData, orDecryptedData*

```
function ENCRYPTDECRYPT($userData$)
    A=$CreateMatrix(tokenId, userId, correlationId, order)$
    K=$GenerateKey(A)$
    $N \leftarrow length(data)$
    for $k \leftarrow i = 1$ to $N$ do
        $result[i] = data.charAt(i) \oplus$ key.charAt(i $mod$ (key.length -1))
    end for
    return $result$
end function
```

5. PROPOSED ARCHITECTURE

As we defined an approach, we aims to propose secure and privacy-aware data collection solution architecture.

5.1. Our proposition

We propose a secure and privacy-preserving data collection architecture (cf. figure 3) based on:

- IOT identity management at device level: each device should send data first to a fog. All authentication, authorization, revocation and accountability process are managed on the fog node. Devices are authenticated by Id which is changing by the time, IP and MAC address. All unknown devices are revoked. Device recover process must be implemented for those which have an ID duration has expired.
- Privacy-aware data collection on the Fog Nodes: Shared key is generated according to token Id, and an order specified for each request, then data is encrypted using Xor operation before transmission on the network.
- Data decryption and processing on the cloud servers: using online the shared key based on token Id and an order in the response from fog node, the application on server side can decrypt data. Thus, privacy for all sensitive data are preserved.

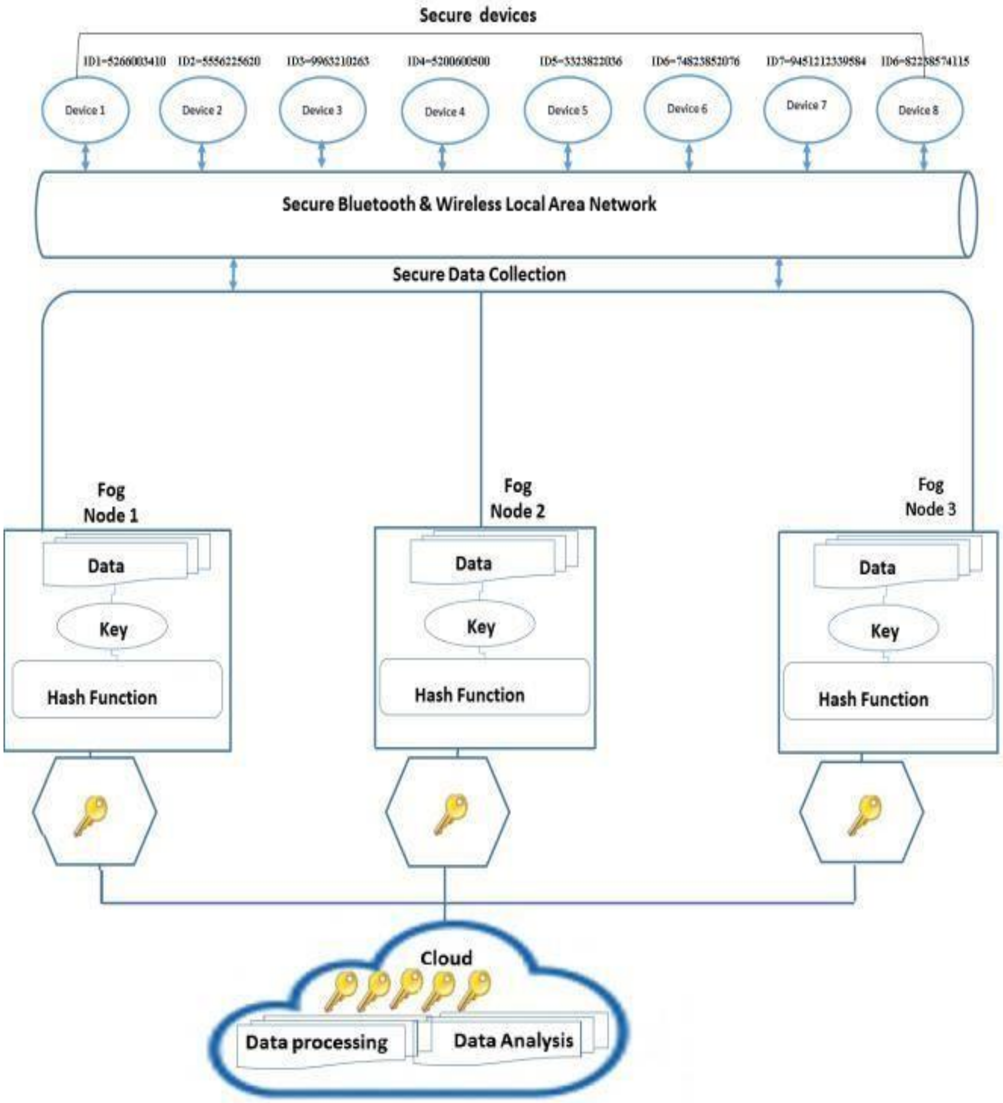
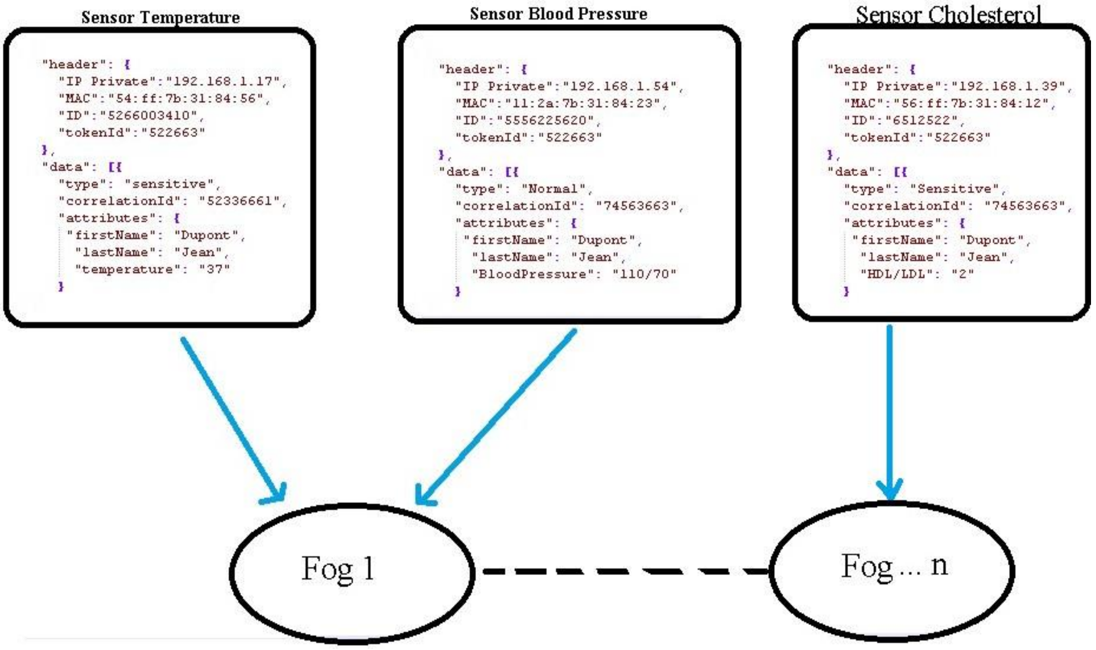


Figure 3: Proposed architecture

5.2. Prototyping And Implementation

We have implemented proposed solution using iFogSim [9] in Eclipse. To simplify our model, we assume that sensors exchange JSON format message. We implemented a fog platform to collect data from many devices. We created several broker, fog and edge devices using iFogSim and CloudSim toolkit.



```
"header": {
  "IP Private":"192.168.1.17",
  "MAC":"54:ff:7b:31:84:56",
  "ID":"5266003410",
  "tokenId":"522663"
},
"data": [{
  "type": "sensitive",
  "correlationId": "52336661",
  "attributes": {
   "firstName": "Dupont",
    "lastName": "Jean",
    "temperature": "37"
  }
```

```
"header": {
  "IP Private":"192.168.1.54",
  "MAC":"11:2a:7b:31:84:23",
  "ID":"5556225620",
  "tokenId":"522663"
},
"data": [{
  "type": "Normal",
  "correlationId": "74563663",
  "attributes": {
   "firstName": "Dupont",
    "lastName": "Jean",
    "BloodPressure": "110/70"
  }
```

```
"header": {
  "IP Private":"192.168.1.39",
  "MAC":"56:ff:7b:31:84:12",
  "ID":"6512522",
  "tokenId":"522663"
},
"data": [{
  "type": "Sensitive",
  "correlationId": "74563663",
  "attributes": {
   "firstName": "Dupont",
    "lastName": "Jean",
    "HDL/LDL": "2"
  }
```

Figure 4: Prototype design

5.3. Data Encryption/Decryption Performance Analysis

We assess the performance of our proposed scheme (cf. subsection 4.4) comparing with AES algorithm. We can see that our scheme provide key generation from element conveyed in data and encrypting/decrypting process is more performant that AES as shown in the following picture.

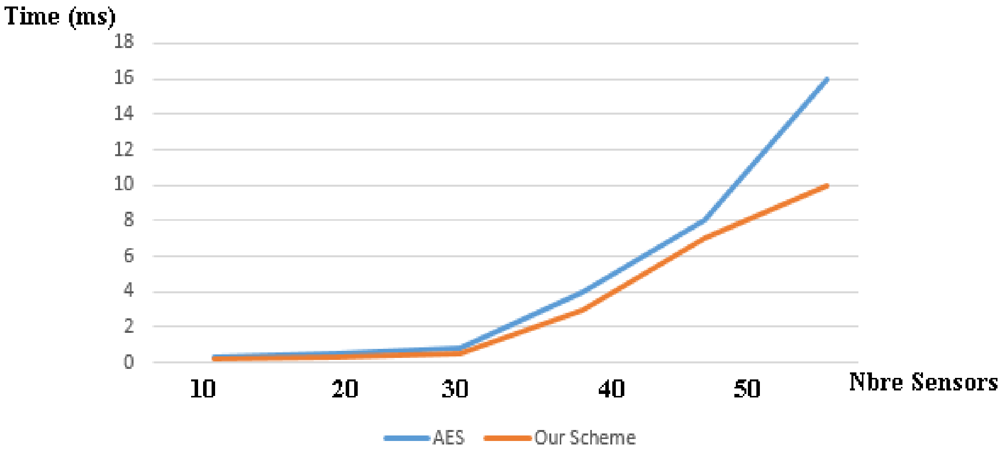


Figure 5: Our scheme vs AES performance analysis

6. Discussion and Analysis

Maintaining security and privacy in IOT enabled platform becomes more difficult. Security and privacy requirements in IOT enabled architecture should be implemented along multi-layers:

- Securing device at the perception layer

- Securing the transport channel at the network layer
- Secure databases, files systems, and business applications at application layer

6.1. Discussion

The proposed architecture provide device security and preserve data integrity and confidentiality. All IOT devices are authenticated and their ID are management with possible revocation. A shared key generation mechanisms will encrypt data. Device traceability are guaranteed. A token ID is generated for each request. Device should be trusted by applying all mechanisms used to identify and recognize a component as trust and secure to communicate with other applications within IOT platform. Data should also be trusted using process to ensure that the data has never been altered during transport on the network. We should ensure that data should be identical from the source.

Device resilience refers the ability of a component to maintain service with alteration in the system environment while robustness refers to its resilience against attacks.

Thus, Data integrity and confidentiality are preserved. This solution prevent against Spoofing and Man in the middle attacks. Generated shared key based on token ID and an order will be different for each request.

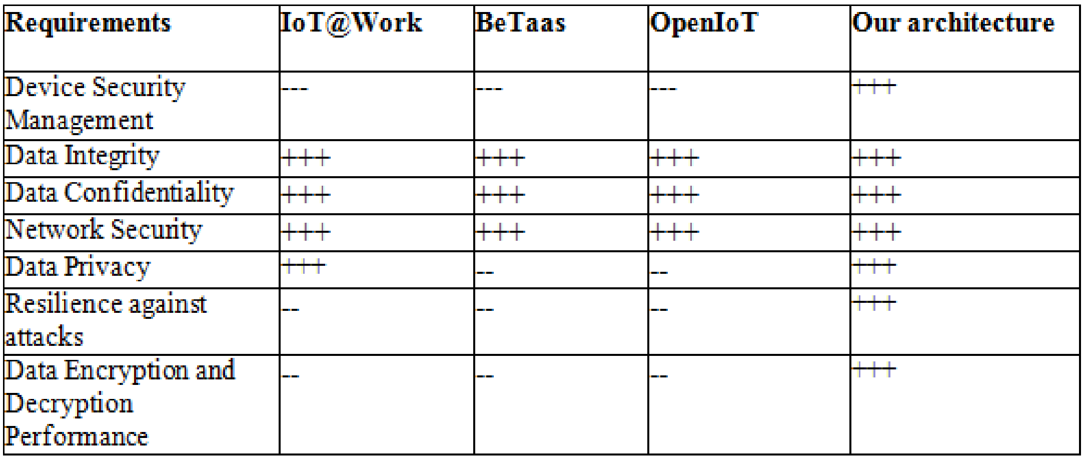
A malicious attacker cannot access to device ID which is changing by the time (cf. section 4.1). The data encryption preserve data integrity and confidentiality. Data privacy are guaranteed in our architecture. Thus, the proposed model provides data privacy policies and device security and resiliencies against malicious attacks.

A malicious attacker cannot access to device ID that is changing by the time. The data encryption preserve data integrity and confidentiality and preserve data privacy comparing with other IOT architecture in the literature. Comparing with other IOT architectures, the proposed model provide data integrity, data confidentiality, data privacy policies, and device security and resiliencies against malicious attacks.

6.2. Comparison Analysis

We conducted a comparative analysis of the proposed architecture against other well-known framework (see Table 2) such as IoT@Work, BeTaa and OpenIoT. We remark that our and IoT@Work architecture are data privacy.

Table 2. Our proposition vs other IOT architecture.



Requirements	IoT@Work	BeTaas	OpenIoT	Our architecture
Device Security Management	---	---	---	+++
Data Integrity	+++	+++	+++	+++
Data Confidentiality	+++	+++	+++	+++
Network Security	+++	+++	+++	+++
Data Privacy	+++	--	--	+++
Resilience against attacks	--	--	--	+++
Data Encryption and Decryption Performance	--	--	--	+++

7. Conclusions and Future Work

In this paper, we proposed a new architecture based on shared key generation and data encryption on fog and cloud IOT enabled environment. Data integrity, data confidentiality and data privacy are preserved by data encryption mechanisms. Device are authenticated and authorized. IoT Device Identity Management process ensure traceability and revocability. The proposed architecture prevent malicious attacks such as Spoofing and Man in the middle attack. In the future work, we are planning to implement a real-life use case to assess security, data confidentiality preservation and performance in fog and cloud IOT-enabled distributed environment.

References

[1] Aaditya Jain, B. S. (2016, April). Internet of Things: Architecture, security goals, and challenges. International Journal Innovative Research in Science & Engineering (IJIRSE), Vol.No2:Issue4

[2] Alfaqih, T. M., & Al-Muhtadi, J. (2016). Internet of Things Security based on Devices Architecture. International Journal of Computer Applications (0975 – 8887).

[3] Bawany, N.Z.; Shamsi, J.A.: Application layer DDoS attack defense framework for smart city using SDN. In: Computer Science, Computer Engineering, and Social Media (CSCESM) (2016)

[4] Botta, A.; de Donato, W.; Persico, V.; Pescapé, A. Integration of Cloud computing and Internet of Things: A survey. Future Generation Computer Systems 2016, 56, 684–700.

[5] Chaqfeh, M.A.; Mohamed, N. Challenges in Middleware Solutions for the Internet of Things. In Proceedings of the 2012 International Conference on Collaboration Technologies and Systems (CTS), Denver, CO, USA, 21–25 May 2012; pp. 21–26.

[6] Elmaghraby, A. S., and M. M. Losavio. 2014. Cyber security challenges in Smart Cities: Safety, security and privacy. Journal of Advanced Research 5 (4): 491--497.

[7] Frank D. McSherry, Privacy integrated queries: an extensible platform for privacy-preserving data analysis, Proceedings of the 2009 ACM SIGMOD International Conference on Management of data, June 29-July 02, 2009, Providence, Rhode Island, USA

[8] Fried, C.: Privacy. The Yale Law Journal Vol. 77, No. 3. (1968) p. 486. p. 475

[9] Harshit Gupta, Amir Vahid Dastjerdi, Soumya K Ghosh, and Rajkumar Buyya. 2016. iFogSim: A Toolkit for Modeling and Simulation of Resource Management Techniques in Internet of Things, Edge and Fog Computing Environments. arXiv preprint arXiv:1606.02007 (2016).

[10] Hay M. , Kun Liu , G. Miklau , J. Pei , E. Terzi, Privacy-aware data management in information networks, Proceedings of the 2011 ACM SIGMOD International Conference on Management of data, June 12-16, 2011, Athens, Greece

[11] Jamil, D., and H. Zaki. 2011. CLOUD COMPUTING SECURITY. International Journal of Engineering Science and Technology 3 (4): 3478--3483. ProQuest SciTech Collection.

[12] Lazarescu, M.T. Design of a WSN Platform for Long-Term Environmental Monitoring for IoT Applications.IEEE J. Emerg. Sel. Top. Circuits Syst. 2013, 3, 45–54.

[13] Majtényi L.: Az információs szabadságok: adatvédelem és a közérdekű adatok nyilvánossága. Complex, Budapest, 2006. p. 211. Simon 2005. pp. 33-34.; Szabó 2005. p. 45.

[14] Maram, B., Gnanasekar, J.M., Manogaran, G. et al. Service Oriented Computing and Applications March 2019, Volume 13, Issue 1, pp 3–15

[15] Machanavajjhala A., Gehrke J., Kifer D., Venkitasubramaniam M. l-diversity: Privacy beyond k-anonymity. 22nd International Conference on Data Engineering (ICDE'06), 24-24

[16] Ndibanje, B., H.-J. Lee, and S.-G. Lee. 2014. Security Analysis and Improvements of Authentication and Access Control in the Internet of Things. Sensors (Basel, Switzerland) 14 (8): 14786--14805. Pmc.

[17] Nissenbaum, H.: Protecting Privacy in an Information Age: the Problem of Privacy in Public. Law and Philosophy Vol. 17, No. 5-6. (1998) p. 581.

[18] Ricardo Neisse, G. S. (2015). A Model-based Security Toolkit for the Internet of Things. ScienceDirect.

[19] Roman R., Zhou J., and Lopez J., “On the features and challenges of security and privacy in distributed internet of things,” Computer Networks, vol. 57, no. 10, pp. 2266–2279, 2013.

[20] Nakamura E.T., Ribeiro S.L., Privacy A, Security, Safety, Resilience and Reliability Focused Risk Assessment In a Health IoT System : Results from OCARIoT Project. IEEE Global Internet of Things Summit (GIoTS), June 2019.

[21] Wang R, Zhu Y, Chen TS et al. Privacy-preserving algorithms for multiple sensitive attributes satisfying t-closeness. Journal of Computer Science and Technology, 2018, Volume 33, Number 6, Page 1231

[22] Weber R. H., “Internet of things–new security and privacy challenges,” Computer law & security review, vol. 26, no. 1, pp. 23–30, 2010.

[23] Westin, A. F.: Social and political dimensions of privacy. Journal of Social Issues Vol 59, No. 2. (2003) pp. 431-434.

[24] Samarati P. & Sweeney L., Protecting Privacy when Disclosing Information: k-Anonymity and its Enforcement through Generalization and Suppression. Technical Report SRI-CSL-98-04. Computer Science Laboratory, SRI International.1998.

[25] Sicari S., Rizzardi A., Grieco L.A., Coen-Porisini A., Security, privacy and trust in Internet of Things, Computer Networks: The International Journal of Computer and Telecommunications Networking, v.76 n.C, p.146-164, January 2015.

[26] Solove, Daniel J., «Conceptualizing Privacy» (2002) p. 1094.

[27] Xiao L, H. B. (2010). A knowledgeable security model for distributed health information systems. Computers & Security., (pp. 331-349).

[28] Xi-Jun Lin , Lin Sun , Haipeng Qu, Insecurity of an anonymous authentication for privacy-preserving IoT target-driven applications, Computers and Security, v.48 n.C, p.142-149, February 2015.

[29] Xin Ma, Q. H. (2010). Study on the Applications of Internet of Things in the Field of Public Safety. China Safety Science Journal, 20(007):170-176.

[30] Yang X., Z. L. (2012). "A multi-layer security model for internet of things," in Internet of Things. Springer, 388-393.

[31] Yunjung Lee, Y. P. (2015). "Security Threats Analysis and Considerations for Internet of Things". 2015 8th International Conference on Security Technology (SecTech), (pp. vol. 00, no., pp. 28-30).

[32] Zhang W., B. Q. (2013). Security Architecture of the Internet of Things Oriented to Perceptual Layer. in International Journal on Computer, Consumer and Control (IJ3C), Volume 2, No.2.

[33] Zhiqiang Yang, S. Z. (2005). Anonymity-preserving data collection. In Proceedings of the eleventh ACM SIGKDD international conference on Knowledge discovery in data mining (KDD '05). ACM, New York, NY, USA, (pp. 334-343).

[34] Ziegeldorf J.H., Morchon O.G., Wehrle K. Privacy in the Internet of Things: Threats and challenges Security and Communication Networks, 7 (12) (2014), pp. 2728-2742

AUTHORS

Moussa WITTI is a consulting engineer and IT architect in the R&D. He is advising bank and insurance firms in content and data management. He has more than 13 years of IT application development and deployment experience. He has obtained an MBA from Toulouse Business School and master Research in Computer Science from university of Franche-Comté in Besançon (FRANCE).

Dimitri Konstantas is Professor at the University of Geneva (CH) and director of the . He has been active since 1987 in research in the areas of Object Oriented systems, agent technologies, and mobile health systems, with numerous publications in international conferences and journals. His current intersts are Mobile Services and Applications with special focus in the well-being services for elderly and information security.Prof. Konstantas has a long participation in European research and industrial projects and is consultant and expert to several European companies and governments.