UTM UNIVERSITI TEKNOLOGI MALAYSIA
INTERNATIONAL JOURNAL OF INNOVATIVE COMPUTING
ISSN 2180-4370
Journal Homepage : https://ijic.utm.my/

Hybrid Encryption for Messages' Confidentiality in SOSE-Based IOT Service Systems

Musa Midila Ahmed
Physical Science Education Department
Modibbo Adama University,
Yola, Nigeria
Email: ahmedmm4me@yahoo.com

Submitted: 23/2/2021. Revised edition: 5/7/2021. Accepted: 11/7/2021. Published online: 15/11/2021
DOI: https://doi.org/ 10.11113/ijic.v11n2.292

***Abstract*—Internet of Things (IOT) is an essential paradigm where devices are interconnected into network. The operations of these devices can be through service-oriented software engineering (SOSE) principles for efficient service provision. SOSE is an important software development method for flexible, agile, loose-coupled, heterogeneous and inter-operable applications. Despite all these benefits, its adoption for IOT services is slow due to security challenges. The security challenge of integration of IOT with service-oriented architecture (SOA) is man-in-the-middle attack on the messages exchanged. The transport layer security (TLS) creates a secured socket channel between the client and server. This is efficient in securing messages exchanged at the transport layer only. SOSE-based IOT systems needs an end-to-end security to handle its vulnerabilities. This integration enables interoperability of heterogeneous devices, but renders the system vulnerable to passive attacks. The confidentiality problem is hereby addressed by message level hybrid encryption. This is by encrypting the messages by AES for efficiency. However, to enable end-to-end security, the key sharing problem of advanced encryption standard (AES) is handled by RSA public key encryption. The results shows that this solution addressed data contents security and credentials security privacy issues. Furthermore, the solution enables end-to- end security of interaction in SOSE-based IOT systems.**

***Keywords*—Hybrid Encryption, Message Confidentiality, SOSE-Based IOT, IOT Service Systems, SOSE**

I. INTRODUCTION

In recent years, IOT emerges as an essential paradigm where devices are interconnected into network. These devices can be operated directly in response to the environment or through programs for efficient service provision [1]. The basic concepts of IOT according to the authors is the optimal utilization of available objects and things. IOT is an intelligent systems, which comprises network of intelligent objects interconnected and communicates with each other to provide services in many fields. IOT according to [2] is a world of physicals devices that are integrated into network and participates actively in business processes. The main problem in IOT technology is to enable interoperability between heterogeneous interconnected devices. A proposed solution to this heterogeneity problem by [3] is the integration of IOT with service-oriented architecture (SOA).

SOSE is a subset of software engineering that focused on application development by integration of autonomous services. The SOSE systems' automated and dynamic interactions capability between sender and receiver is crucial in provision of robust IT solution for modern industries. According to [4], the future development of SOA will lead to autonomous services' collaborations for efficient global business processes. Nowadays, companies and business organizations that integrated this vital technologies have excelled beyond their competitors. In the implementation of SOA, service descriptions are published in form of web service description language (WSDL) in universal, description, discovery and integration (UDDI) as shown in Fig. 1. Functionalities are discovered by the receiver in the UDDI as described in the senders' WSDL. The sender published the WSDL of their services in the UDDI. The receiver choice and bind to the service that suits their needs as described by the WSDL. The sender and receiver interact to-and-fro by SOAP messages' exchange. The SOAP envelope is writing in XML language.

Basically, SOA implementation involves three interacting entities, a producer (or sender, or responder) of service, a consumer (or receiver or requester) of service and a broker (or registry or directory) of available services. An internal or external service producer publishes a list of its services to the broker. The consumers' application queries the broker to find its required service. The broker supplies the required services' access information to the consumer application. Finally, the consumer application request the service directly from the producer. The producer on satisfaction with the consumer applications' request authorizes it to use the specified service.

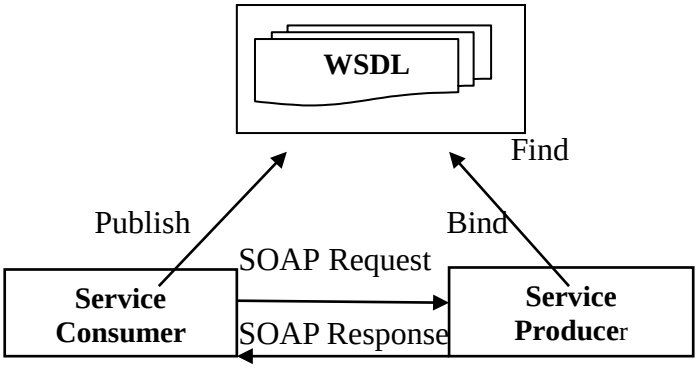


Fig. 1. SOSE service implementation

A. IOT Services

Internet is a global interconnected networks of devices by using standard communication protocols. The connected devices such as computers, smartphones, and tablets are identified on the internets by a unique identifiers called an IP address. A device is identified by its IP address number for the internet traffic to locate and route data to the device on the network. Any physical things either object or device with an IP address can be connected to send/receive data on a network. Things that can be connected to the internet include animals, sensors, cameras, tablets, vehicles, smartphones etc. The connection of things with internet results in an emergence of powerful technology called internet of things (IOT).

According to [5], the four fundamental components of IOT as applications, processors, gateways, sensors and actuators. These devices are identified on a large network by their uniquely identifiable IP addresses. Applications provide control interface and effective meaning to the data collected. It is essential for efficient utilization of all data collected and a delivery point for services. Processors process the data collected by the sensors in the IOT system as controlled by the applications. Gateways routes processed data to its proper destination. It provides network connectivity to data essential for any IOT system. Finally, Sensors collect data from the surroundings, while actuators gives out data to the surroundings. IOT service enables integration between physical objects with its changing environment. For instance, an integration of IOT service with entities to sense the temperature of the things and store the temperature value [6].

The basic architecture of IOT according to [7] is the three layers architecture. The three layers according to the author are perception, network and application layers. The perception layer gathers information by physical sensing of the objects' surrounding. The network layer connects these smart objects as well as transmits and processes sensor data. Finally, the application layer delivers specific services to users in form of smart homes, smart offices and smart cities. However, due to the meticulous nature of research, the three layer architecture is not sufficient for IOT research. Consequently, [8] proposed a five-layer architecture of the IOT to help in understanding its essence. The five layers are perception, transport, processing, application and business layer. Perception and application performs the same role as in the three-layer architecture. Transport layer transmits sensor data from the perception layer to the processing layer. The processing layer is the middleware that stores, analyzes and processes data collected from the transport layer. Lastly, business layer which handles the entire IOT systems operations including its security and privacy.

B. SOA and IOT

IOT is a heterogeneous network of variety of things. This makes it difficult for IOT systems' satisfy non-functional requirements such as dynamic systems, flexibility, loose-coupling, scalability and robustness simultaneously [9]. A study in the area of IOT by [6] shows that services play a crucial role in the IOT. Consequently, services are the building blocks of both IOT and service-oriented architecture (SOA). In an effort by the authors to bridge the gap between the enterprise SOA and the physical devices leads to integration of SOA with IOT. The integration of SOA with IOT systems evolved from the need of a middleware to encapsulate the network details from applications. Furthermore, this enables the development of sophisticated systems by providing supports for heterogeneity and interoperability of connected devices.

SOA-based IOT middleware requires the support of security architecture in view of the massive volume of data that passes through the IOT middleware. The middleware according to [10] becomes a security vulnerability point for the system. Although the IOT system has its own security architecture designed for specifically for IOT systems. However, these security architectures cannot be used for the implementation of security standards for confidentiality in SOA-based IOT systems. The price of integration of SOA as the middleware for IOT to leverage its loose-coupled and heterogeneous data transformations nature is additional security challenges.

II. SECURITY CONCERNS

Traditionally, the aim of application security is to protect websites and other online services from exploiting applications' vulnerabilities to launch attacks. Failure by an organization to adequately protect its systems from security threats risks being attacked. Recently, the integration of IOT with SOA brings additional security problems. This is because the TLS that provides security services for communications on the internet uses transport layer protocol. In TLS, client and server applications creates a reliable connection between them to communicate in both direction as shown in Fig. 2. TLS provides internet communications security services on the TCP transport layer protocol. TCP creates a virtual pipeline connections between two systems to transfer data through a sending and receiving buffers. However, SOA is designed to provide services at the application layer for agility, flexibility and efficiency. In typical SOSE implementations, messages passes across mediators while on transit from the sender to the receiver as shown in Fig. 3. Modern organizations need efficient security services to safeguard its applications comprehensively. Therefore, SOSE-based IOT systems requires adequate messages' confidentiality on transit from the sender to the receiver across all intermediaries.

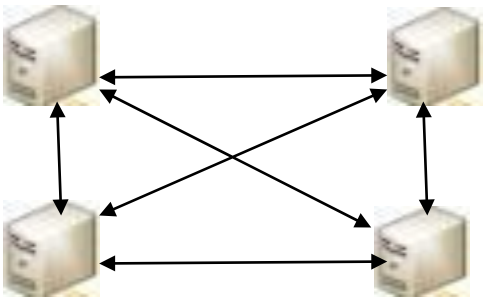


Fig. 2. TLS connections

The movement of data in the sending buffer and receiving buffer is in one direction for each interaction. Currently, TLS is the most prominent security protocol for providing security at the transport layer. However, TLS relied on connection-oriented transport protocol, which creates data queue at the sending buffers and the receiving buffers. This protocol has a performance overhead in establishing connection between the client and the server. Moreover, TLS is slower because it keeps data in the buffer until an acknowledgement is received before establishing the reliable connection between the client and server.

There is the problem of establishing many direct connection between client and server in TLS security services. Particularly, if the number of nodes exceeds three, the number of connections is greater than the number of nodes as shown in Table 1. The performance of the systems is negatively affected by the increase in the number of applications connected. For instance, there are 45 connections for integrating 10 applications and integrating 20 applications results in up-to 290 connections. Imagine the number of connection requires to integrate a million applications. Clearly, the performance of the systems will be slow on integration of millions of application and the vision is to have billions of connected applications in the systems.

TABLE 1. ANALYSIS OF TLS CONNECTIONS

N	C= N(N-1)/2	Remarks
2	1	No. of Connections < No. of Nodes
3	3	No. of Connections = No. of Nodes
4	6	No. of Connections > No. of Nodes
5	10	No. of Connections > No. of Nodes
10	45	No. of Connections > No. of Nodes
20	190	No. of Connections > No. of Nodes
100	4,950	No. of Connections > No. of Nodes

With the enterprise service bus (ESB) at the heart of SOSE systems that enables protocol and format transformation of messages. The system will be more scalable, flexible, agile and efficient. It will be scalable because the number connections is equal to the number of nodes for whatever number of nodes. Furthermore, the system supports interoperability of heterogeneous devices as well as becomes easy to troubleshoot and maintained. Governance of security services are easily formulated at the center for compliance by all connected devices as shown in Fig. 3.

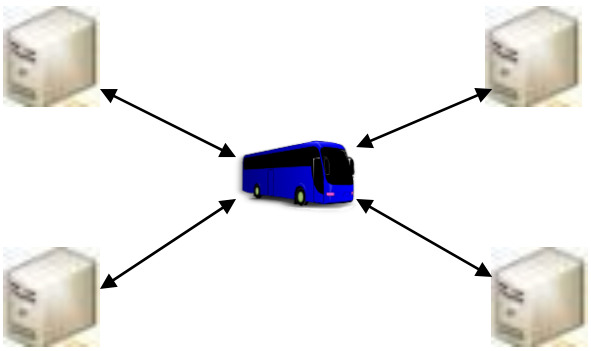
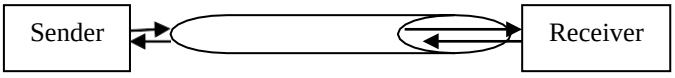


Fig. 3. SOA connections

SOSE supports transformations of messages protocol and format to enable heterogeneous communication between integrated devices. SOSE system enable end-to-end communications since all connected devices interacts through the ESB. Any maintenance and troubleshooting can easily be effected and devices can easily be added or removed from the ESB interface. The performance of the system remains constant irrespective of the number of devices connected. This is because each device is connected to the ESB as such establishing an indirect connection between all devices. However, despite all these benefits, SOSE innovation introduced new security challenges.

The challenge in enforcing security in SOSE-based IOT system is that the TLS protocol reads inputs and write outputs as data streams. Basically, data streams is like a pipeline. Information are loaded into the pipeline and extracted out of the pipeline as shown in Fig. 4.



Fig, 4. The TLS Data Stream Pipeline

However, SOSE-based IOT systems has one or more mediators that transform messages as shown in Fig. 5. The reading input and writing output of the data stream pipeline repeats at the intermediaries. This leads to confidentiality problems in the system, since the transmitted messages would be exposed to the intermediaries. This type of attack is generally referred to as man-in-the-middle attack. It appears to the communicating parties that normal exchange of information is on-going. However, impersonators might gain access to the information that the sender and the receiver exchanges.

Fig. 5. TLS in SOSE-Based IOT System

According to [11], man-in-the-middle attack is broadly classified into active attacks and passive attacks. Active attacks refers to unauthorized modification of messages' content. Whereas passive attacks only monitors the transmitted data for useful information. This paper focused on the solution of passive attacks in SOSE-based IOT systems. Although passive attacks does no harm to the messages on transit. It is a threats against the confidentiality of the transmitted data. Passive attacks are of two types; the data content attack and credential attack.

The data content attack is a type of passive attack in which the attackers' aimed at getting transmitted information. The attackers' goal is to understand the contents of telephone conversation, electronic mail messages or transferred files, etc. that might contain sensitive information. Therefore, security services should prevent the mediators from understanding the contents of transmissions. The credential attacks aimed at getting useful information from the transmitted data for determining the nature of communications. The attacker might determine the location or identity of the communicating parties. Furthermore, information such as frequency of messages and length of messages being transmitted should be clues for launching active attacks.

III METHODOLOGY

The aim of confidentiality is to protect messages from exposure to mediators. In other word, confidentiality principles protects the privacy of the communicating parties. Therefore, security services must ensure that confidential information is protected from unauthorized exposure to the mediators while on transit. This is important to safeguard the identity credentials of communicating parties and sensitive data from being exploited to attackers. Confidentiality can be achieved by encryption of all sensitive data both on transit and at rest. Encryption scrambles the transmitted data making it unreadable to unauthorized parties. This prevents malicious parties from accessing and understanding sensitive transmitted data.

A. Selection of Method for Confidentiality

Confidentiality of data both at rest and on transit can be achieved by encryption. Generally, there are two categories of encryption; symmetric encryption and asymmetric encryption. Symmetric encryption uses the same key for both encryption and decryption. Consequently, there must be a secured way of transmitting the key along with the message to the receiver. This is to enable the receiver decrypt the message with the same key used in encrypting it at the senders' side. The advantages of symmetric encryption is that it uses a huge key size, which provides better security of messages. In addition, it is relatively faster than the asymmetric encryption. However, the major disadvantage of symmetric encryption is that it requires a reliably secured channel for transferring the secret key to the receiver to enable decryption of the message with the same key.

On the other hand, asymmetric encryption uses two distinct keys known as public key and private key. The public key is used for encrypting the messages at the senders' side. Whereas, the private key is used for decrypting the message at the receivers side, which was encrypted by the corresponding public key. The major advantages of asymmetric encryption is that interacting parties has pair of public and private keys for encryption and decryption of messages respectively. Therefore, there is no key sharing requirement in this encryption method. Furthermore, numerous key pairs can be generated adequate for securing huge information systems. The scalability and flexibility of asymmetric encryption enhances its security service efficiency making it suitable for open systems. However, because of the massive calculations in asymmetric encryption renders it slower than symmetric encryption. Another disadvantage of using asymmetric encryption is that the management of public keys requires the service of trusted certificate authority.

i) Justification for use of Hybrid Encryption

Hybrid encryption incorporates the good features of both the symmetric and asymmetric encryption methods for efficiency and effectiveness in securing communications of open systems. Hybrid encryption leverages on the excellent security capability and high speed of symmetric encryption. However, the key sharing weakness of symmetric encryption method is resolved by using asymmetric encryption method for encoding and decoding the secret keys. Furthermore, the expandability of asymmetric encryption method enables the connection of large number of devices in SOSE-based IOT systems. Overall, using hybrid encryption method for confidentiality leads to effective, fast-moving and extensible SOSE-based IOT systems.

Among the symmetric encryptions, advanced encryption standards (AES) is more suitable than data encryption standards (DES). The security of DES is not enough to adequately protect information systems. This problem leads to increase by tripling of its key size and rounds where 3DES evolved. Unfortunately, the speed of 3DES is very slow because of its enhanced key with large number of rounds. The efficiency of AES is a results of its enhanced key and block size with lower number rounds. This results in AES's high speed and excellent security service provision. However, despite the high speed and excellent security provision of AES symmetric encryption, it needs a secured means of transferring the secret key from the sender's side to the receiver's side.

Among the asymmetric encryptions, RSA is found better than Diffie-Hellman (DH) asymmetric encryption method because of its scalability and good security. The good security of RSA emanated from the difficulty in identifying huge integers that are product of two large prime numbers. The advantage of RSA asymmetric encryption is that communicating parties has a pair of public and private keys. Therefore, there is no need for transferring keys from one end to the other for encryption and decryption. However, RSA has the general weakness of asymmetric encryption of being slower than symmetric encryption methods. Consequently, RSA asymmetric encryption can be used for encryption of AES's secret key. This is because the size of the secret key is small and RSA is scalable convenient for securing large systems. The analysis of hybrid encryption is shown in Table 2.

TABLE 2. HYBRID ENCRYPTION TECHNIQUE

AES Symmetric Encryption	**RSA Asymmetric Encryption**	**Hybrid Technique (AES + RSA)**
i) **Secret Key**: Uses same key for encoding and decoding	i) **Public/Private Key:** Uses distinct key for encoding and decoding	i) **Public/Private Key:** Uses distinct key for encoding and decoding
ii) **Key Sharing Required**: The same key used for encoding must be use for decoding	ii) **No key sharing**: Public key is use for encoding and private key use for decoding	ii) **No key Sharing:** Public key is use for encoding and private key use for decoding the secret key
iii) **Excellent Security**: Used to encryption message content	iii) **Good Security:** Used to encryption secret key	iii) **Very Good Security:** Since message is significantly larger

B. Hybrid Encryption Method

The aim of hybrid encryption method is to enable delivery of messages from the sender to the receiver in such a way that the mediators would not understand its header and content. Precisely, hybrid encryption method protects messages from exposure to the mediators as shown in Fig. 6. Confidentiality of the message is protected by wrapping the AES secret key with RSA public key encryption for its secured transfer to the receiver. This enables the receiver decode the message content with the decrypted secret key by AES encryption method.

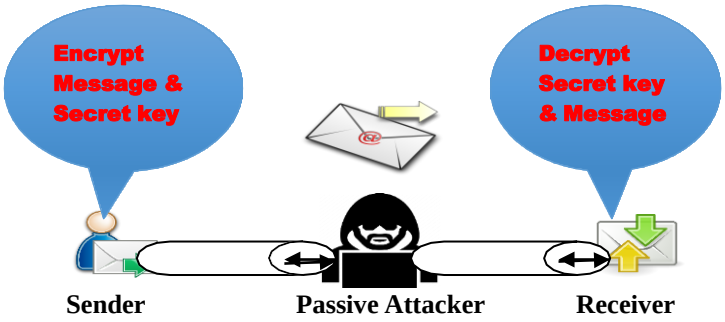


Fig. 6. Hybrid encryption Method

At the senders' side, the sender prepares messages for the receiver and encrypts the message with AES's secret key. Also, encrypts the secret key with the receivers' public key. Then send the encrypted messages to the receiver.

At the receivers' side, the receiver on getting the envelope decrypts the AES's secret key with his private key and finally decrypts the message with the decrypted AES secret key. This enables secured data transmission across all intermediaries.

IV. RESULT AND DISCUSSION

This section presents the results of the experiment. It describes the results by the analysis of the data collected from the experiment. It is organize in three (3) subsections; section A presents the experimental results. This include analysis of SOAP request and response. Followed by section B for advantages and disadvantages of the method. Section C is for discussion of the experimental results.

A. Experimental Results

This subsection summarized the findings of the study. Exchange of messages in SOA-based IOT implementation is in SOAP envelope using XML language. In this experiment, the SOAP envelope contains adequate encryption indicators. XML encryption in SOAP envelope ensures confidentiality of the messages in transit [12]. This encryption technique preserves the confidentiality of messages across all mediators.

Analysis of the outcome of this experiment shows that an encrypted SOAP messages with encrypted key and the encrypted data element was created. The content of the SOAP envelope shows proper XML encryption of the secret key. The method of encryption of the key was adequate as shown by the cipher data and key information in the SOAP messages. It was observed that RSA public key encryption is the method used for encryption of the keys. Furthermore, the SOAP envelope shows proper XML encryption of messages' content. The method used for encryption of the key was adequate as shown by its cipher data and key information. AES encryption was observed as the method for encryption of the messages' content.

This process encrypts the AES's secret key by wrapping it at the senders' side and unwraps it at the receivers' side. In a nutshell, RSA encryption handles the confidentiality of the secret keys by transmitting it in secure manner from the sender to the receiver. This ensures only the holder of the RSA private key can decrypt and get access to the secret keys. On the decryption of the secret keys, the receiver uses it to decrypt the message contents.

B. Advantages and Disadvantages of the security solution

This subsection is for advantages and disadvantages of the hybrid encryption method for confidentiality of messages in SOSE-based IOT system. This is to assess the robustness and deficiency of this approach for confidentiality.

i) Advantages of the Hybrid Encryption Method

- This approach prevents mediators' understanding of both the messages' content and heading.
- This method provides confidentiality for the vital aspects of the messages making it harder to attack.
- It reinforces security suitable for heterogeneous interactions in an open systems.
- It is built on open standards adequate for security enforcement in distributed heterogeneous systems.

ii) Disadvantages of the Hybrid Encryption Method

- It requires certificate authority for management and distribution of asymmetric keys.
- Mediator is required to serve as the gateway for security enforcement, which renders the system vulnerable to attacks.

C. Discussion of Findings

This subsection discusses the consequences of implementation of the hybrid encryption method. This approach resolves the data content attack and credentials attack in SOSE-based IOT systems.

i) Credential Security

The aim of attackers in this approach is to obtain the credentials of the communicating parties. The attackers focuses on analysis of the traffic with the aim of decoding the secret keys of interacting entities [13]. The hybrid encryption secured the credentials of communicating parties as follows. First, the secret keys was wrapped at the senders' end, transmitted across all intermediaries encrypted and unwrapped at the receivers end. This ensured a secured secret keys exchange between the sender and the receiver. Second, the generated interaction keys expired after 300 milliseconds. This leaves the attackers with little time not enough to identify the keys for any particular interaction. Finally, this solution used a timestamp of 300 milliseconds for all messages. As such all messages that lasted more than 300 milliseconds was discarded.

ii) Data Content Security

Effective communication requires only the sender and the receiver understands messages' content. The aim of attackers is to understand the content of transmitted data [14]. This approach optimizes secured interactions between messages sender and its recipient in a meaningful manner. This method ensures that the mediators is unable to decode the contents of messages on transit by encoding it with an efficient encryption method.

V. SUMMARY AND CONCLUSION

IOT is an integration of physical devices into network, which participates actively in business transactions. IOT is integrated with SOA to enable interoperability of heterogeneous devices. To enable interoperability between heterogeneous interconnected devices leads to integration of IOT with SOA. SOSE is a software development method by composition of reusable services. Messages in SOSE implementation are sent and received in SOAP envelopes. The sender creates an XML messages in SOAP format for the receiver. Conversely, the receiver reacts in SOAP envelope to the sender's WSDL specified in XML format. In a nutshell, on successful establishment of connection, the sender and receiver interacts to-and-fro in SOAP format.

The integration of IOT with SOA brings confidentiality security problem. This security issues surface due to the mediators' role of dynamically changing messages' format and protocol enabling heterogeneous interactions between various things. The TLS protocol can only secure direct communication routes by creating a safe virtual pipeline between the sender and the receiver of messages. However, the dynamical transformation of messages that passes through the mediators in SOSE-based IOT renders the system vulnerable to attacks. This paper proposed hybrid encryption technique solution to this problem. In this method, message content was encrypted by AES and the key sharing problem of AES was effected by RSA public key encryption. This techniques enables end-to-end security of interactions between IOT devices. In addition, it resolved the data content attack and credential attack in SOA-based IOT systems. The former was resolved by encrypting the messages with strong encryption algorithms and the latter by encrypting the secret keys with public–private keys to enable key sharing.

REFERENCES

[1] Atzori, Luigi, Antonio Iera, and Giacomo Morabito. (2010). The Internet of Things: A Survey. *Computer Networks.* 54(15): 2787-2805.

[2] Haller, Stephan, Stamatis Karnouskos, and Christoph Schroth. (2008). The Internet of Things in an Enterprise Context. *Future Internet Symposium*. Springer, Berlin, Heidelberg.

[3] Spiess, Patrik, *et al.* (2009). SOA-based Integration of the Internet of Things in Enterprise Services. *2009 IEEE International Conference on Web Services*. IEEE.

[4] Bouguettaya, Athman, Munindar Singh, Michael Huhns, Quan Z. Sheng, Hai Dong, Qi Yu, Azadeh Ghari Neiat *et al*. (2017). A Service Computing Manifesto: The Next 10 Years. *Communications of the ACM.* 60(4): 64-72.

[5] Hussain, Fatima. (2017). *Internet of Things: Building Blocks and Business Models*. No. 978-3. Springer International Publishing.

[6] Thoma, Matthias, Sonja Meyer, Klaus Sperner, Stefan Meissner, and Torsten Braun. (2012). On Iot-services: Survey, Classification and Enterprise Integration. *2012 IEEE International Conference on Green Computing and Communications*. IEEE. 257-260.

[7] Sethi, Pallavi, and Smruti R. Sarangi. (2017). Internet of Things: Architectures, Protocols, and Applications. *Journal of Electrical and Computer Engineering.*

[8] Wu, Miao, Ting-Jie Lu, Fei-Yang Ling, Jing Sun, and Hui-Ying Du. (2010). Research on the Architecture of Internet of Things." *2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)*. IEEE. 5: V5-484.

[9] Yang, Yi, Zhiliang Wang, Quanbin Liu, and Lu Wang.(2012). Building a Pervasive SOA based IOT Communication Middleware using Runtime Compilation and Reflection. *Journal of Computational Information Systems.* 8(2): 643-654.

[10] Tiburski, Ramão Tiago, Leonardo Albernaz Amaral, Everton De Matos, and Fabiano Hessel. (2015). The Importance of a Standard Security Architecture for SOA-based IOT Middleware. *IEEE Communications Magazine.* 53(12): 20-26.

[11] Indrakanti, Sarath. (2012). *Service Oriented Architecture Security Risks and Their Mitigation*. Defence Science and Technology Organisation Edinburgh (Australia) Command Control Communications and Intelligence Div.

[12] Lawrence, Kelvin, *et al.* (2006). Web Services Security: SOAP Message Security 1.1 (WS-security 2004). *OASIS, OASIS Standard, Feb.*

[13] Feghhi, Saman, and Douglas J. Leith. (2016). A First-hop Traffic Analysis Attack against a Femtocell. *2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC)*. 1060-1065. IEEE.

[14] Cho, Jung-Sik, Sang-Soo Yeo, and Sung Kwon Kim. (2011). Securing against Brute-force Attack: A Hash-based RFID Mutual Authentication Protocol using a Secret Value. *Computer Communications.* 34(3): 391-397.