Digital Signature with RSA Public Key Cryptography for Data Integrity in SOSE-Based E-Government Systems

Musa Midila Ahmed
[1]Faculty of Education, Department of Physical Science Education, Modibbo Adama University, Yola, Nigeria
OrcidID: 0000-0002-7769-6400; E-mail: ahmedmm4me@yahoo.com

Area/Section: Information Technology.
Type of the Paper: Applied Research.
Type of Review: Peer Reviewed as per |C|O|P|E| guidance.
Indexed in: OpenAIRE.
DOI: https://doi.org/10.5281/zenodo.5918479
Google Scholar Citation: IJMTS

How to Cite this Paper:
Ahmed, Musa Midila, (2022). Digital Signature with RSA Public Key Cryptography for Data Integrity in SOSE-Based E-Government Systems. *International Journal of Management, Technology, and Social Sciences (IJMTS), 7*(1), 59-70. DOI: https://doi.org/10.5281/zenodo.5918479

International Journal of Management, Technology, and Social Sciences (IJMTS)
A Refereed International Journal of Srinivas University, India.

CrossRef DOI: https://doi.org/10.47992/IJMTS.2581.6012.0177

Disclaimer: The scholarly papers as reviewed and published by the Srinivas Publications (S.P.), India are the views and opinions of their respective authors and are not the views or opinions of the SP. The SP disclaims of any harm or loss caused due to the published content to any party.

Digital Signature with RSA Public Key Cryptography for Data Integrity in SOSE-Based E-Government Systems

Musa Midila Ahmed

[1]Faculty of Education, Department of Physical Science Education, Modibbo Adama University, Yola, Nigeria

OrcidID: 0000-0002-7769-6400; E-mail: ahmedmm4me@yahoo.com

ABSTRACT

Purpose: *SOSE is a novel software paradigm suitable for development of flexible, loose-coupled and end-to-end E-government system. However, the use of this innovation for E-government system is dwindled by security challenge. Apparently, the TLS (transport layer security) solution traditionally applied to protect SOSE-based E-government systems is inadequate since it can only secure point-to-point channels of communicating. Whereas, an end-to-end security protection is necessary to adequately protect SOSE-based applications.*

Design/Methodology/Approach: *Consequently, this paper proposed use of Digital Signature by RSA (Rivest-Shamir-Adleman) public key cryptographic algorithm at the message level to achieve data integrity in SOSE-based E-government system.*

Findings/Result: *The SOAP message content shows adequate formulation of digital signature with appropriate indicators of RSA public key to ensure data integrity. The SOAP message shows that SignedInfo, Signature Value and KeyInfo were formulated correctly. The SignedInfo contains Canonicalization Method, Signature Method and Reference subelements. Also, SignatureValue element has encrypted digest and the KeyInfo element has security token reference.*

Originality/Value: *This security solution integrates many technologies including OASIS's web service security standard and W3C's (World Wide Web Consortium) XML digital signature into SOAP envelope to ensure data integrity for E-government system at the message level.*

Paper Type: *Applied Research.*

Keywords: Digital Signature, RSA Public Key, Cryptography, SOSE, E-Government

1. INTRODUCTION :

E-government is the use information and communication technology (ICT) to enhance interaction efficiency between citizen and government, government and business as well as among government organizations. With the recent popularity of internet and ICT awareness in almost all countries, the use of E-government for service provision is crucial and timely. According to [1], most developed and underdeveloped nations provide online services as well as gather information from citizens through the internet. E-government system improves interaction and transaction among citizens, businesses and governments. Despite the numerous benefits of digital government such as enhanced quality of service delivery, efficiency, transparency, flexibility, etc. Decision to consider adoption of this technology involves trust, accountability and security factors.

Lack of security is one of the major challenge associated with E-government acceptance. Hassan, R. G. et al (2016) [2] discovered that prevention of data leakage is a crucial aspect of information security in E-government systems. This is to ensure that government network is protected from the continuous growing security threats and risks. However, Alsmadi, I. et al (2016) [3] studied the major threats of E-government portals and discovered that lots of vulnerabilities exists in the websites explored. Therefore, robust security measures need to be in place to protect citizens' sensitive information. The security system must ensure that hackers and unauthorized citizens by all means do not have access to information. Basically, citizens trust and expect adequate security set-up in the E-government system to prevent and protect data loss or abuse. E-government is a robust platform for providing comprehensive public transaction to national security protection.

Service oriented software engineering (SOSE) is a new software development approach that enhances the standards of E-government systems. The use of this paradigm results in agile, loose-coupled, flexible and efficient E-government systems. SOSE-based E-government provides a novel technological experiences that enable robust public service development for citizens. Despite the advantages of SOSE-based E-government system, the use of this technology for public service provision is slowed by security challenges. According to Hassan, R. G. et al (2016) [2], e-government supposed to provide reliable information for public services over an open network. Therefore, it requires advanced security protection to mitigate ever-growing threats and risks. The common security threats include key information leakages or identity theft, messages' confidentiality and messages' integrity. It is important to control access to critical government information both on premises ad on the network. E-government systems should ensure secure interactions for reliable activities between government and citizens, government and businesses and among government agencies. In view of the increase on reliance on the internet for service provision, security of information in E-government systems.

In SOSE implementation, autonomous services are "published" by the service provider on the universal description discovery and integration (UDDI) registry in the network. So that service consumers search the registry for services that suits their needs, referred to as "service discovery". Upon identification of suitable service in the registry, the service consumer "bind" to utilize the service as shown in Figure 1. Once a connection is established between service provider and service consumer, the connection is used for messages exchange to-and-fro between in XML format enclosed in SOAP envelopes between them. In other word, service provider publishes the web service description language (WSDL) of their services in the UDDI directory. The UDDI registry host the WSDL of services to enable consumers locate suitable services and bind to interact with the service provider. Messages are sent and received in SOAP format in SOSE implementation. Service consumer creates their mail messages by XML language in SOAP format to the provider. Conversely, service provider prepares the response as a SOAP message written by XML language according to the specifications defined in WSDL. Generally, service providers and service consumers communicates in XML messages to-and-fro between them in SOAP envelopes.

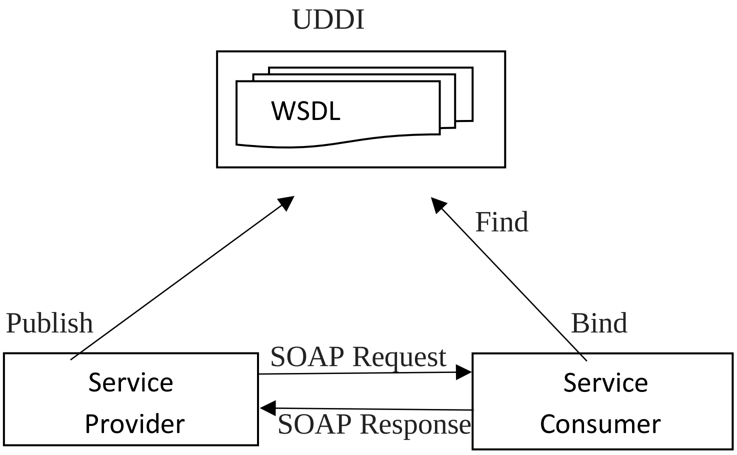

Fig. 1: SOSE implementation

1.1 E-Government Service

E-government is the use of information and communication technology (ICT) to improve public service delivery to citizens. E-government refers to service provision among government agencies as well as between people and governments. Traditionally, ministries, departments and agencies (MDA) located in distant geographical area provides government services by using paper forms. Recently, government services that are delivered digitally is prioritized worldwide. The shift to digital approach of governance by E-government systems has gained acceptance in the developed world. For instance, [4] discovered that the digital service transformation of governance worldwide is toward delivery of all local governments online. The popularity of internet in America is standardized up to the provision of government services and information completely online. Consequently, interactions of Americans government with its citizens is by online channels. However, this is more effective in the region of citizens with highly educational levels and income.

E-government enhances the efficiency and effectiveness of public service delivery by use of modern technology. Furthermore, it is a means of promoting accountability, flexibility, agility and transparency among citizens and government. The internet has transformed the way people interact, learn, and work worldwide. The global internet revolution also transforms the way government service delivery to its citizen, business and other sister government organizations. In a nutshell, E-government refers to the use of ICT for efficient information exchange between government and citizens (G2C), government and business (G2B) as well as among governments (G2G). In other word, E-government enhances information exchange between government sectors (G2G), business services to support governance (G2B) as well as interactions between government and citizens (G2C). This is to enhance the quality governments' service delivery so that citizens can interact and transparently participate in governance easily.

Generally, E-government supports government services to citizens with enhanced interoperability among services to boast performance [5]. The enhancement of the reliance on ICT for public service delivery globally leads to evolution of the concept of e-commerce, e-business and service oriented architecture (SOA). SOA provides flexible, agile, interoperable and autonomous services online that can interact to support the functions of e-governments. The operations of all governments are similar worldwide. Although, it is more complicated for multi-tier government structure. Furthermore, according to [6], the diversity and autonomy of some ministries, departments and agencies of government increases the complexities of the system. Despite governments' huge investment in ICT globally, adequate public service provision remains a challenge. Consequently, further research is required toward novel technologies and architectural models for improving E-government systems.

1.2 SOA and E-Government Service

Nowadays, E-government is an indispensable tool for efficient interaction between government organizations, citizens and businesses. According to Yang, L., [7], E-government system leads to greater transparency and convenience as well as citizen-centred business environment. [8] proposed a practical model for evaluation of public services' business administration in E-government system. The study analysed interactions between government organizations for developing the business model. Similarly, [9] proposed a stable load balancing method for data exchange between eservices. The author focused on design model for integration of legacy system using SOA. [10] evaluated the use of SOA paradigm for implementation of E-government system in Japan. The author adopted SOA ideology to provide a case study of E-government implementation in Japan. A study by [11] proposed an architectural modelling of transport management system for E-government system by SOA. The author uses large cargos to enhance data validation, improve interaction speed and cheaper logistics. [12] examined the best practices for successful SOA governance using semi-structured interview of senior managers in Saudi E-government programme. The qualitative study discovered that additional effort is required for successful adoption of E-government system.

An effort to find solution for heterogeneity and interoperability of E-government system by [13] used Extract-Transfer-Load (ETL) process and SOA to design a flexible and interoperable database for E-government. Similarly, [14] proposed an interoperable E-government architecture using enterprise architectural communication framework based on online interaction of citizens for transformation of E-government systems. An overview of the required digital services and digital interaction of parties in E-government system by [15] provides a comprehensive description of the mediator layers for E-government implementation by SOA. [16] proposed an e-commerce model using business process executive language (BPEL) layer based on SOA to handle citizens complains for Sri Lanka. It is well known that TOGAF (The Open Group Architectural Framework) proved adequate service innovation for good government governance. [17] used TOGAF SOA approach for integrating business process in E-government system by performance analysis of government offices. Also, [18] used web services Architecture to optimize the service procedures running in E-government system. The author proposed an SOA-based framework for integration and interoperability of services in E-government system.

In an effort to unite E-government services, [19] used e-readiness evaluation framework for integration of existing services. The author discovered that legal, governance and human resource requirements be satisfied in E-government systems designs. Another approach by [20] used RESTFUL web service technology for integration of both internal and external services by enterprise service bus (ESB) to transform peer-to-peer (P2P) system into a single large public service system. The author recommends ESB as a suitable middleware for integration of E-government system. Similar focus on integration of government services by [21] used government service bus (GSB) for the management of E-government system. The author use this approach to integrate government-to-business (G2B), government-to-citizens (G2C) AND government-to-government (G2G) services for a smart city system. Also, [22] designed public service model by ESB technology that handles the heterogeneity problem in Indonesian E-government system. The SOA solution is designed by service-oriented design and analysis for integration of Indonesian government services.

Another study by [23] used SOA to integrate independent public services systems in Sidoargo Regency. The study focused on integration of regional government in three phases; database formation, service formation, and service implementation to provide a high speed E-government system. Whereas [24] proposed one-factor user communication model for efficient interaction of citizens and government in SOA-based E-government system using ethno-based analysis of information flow and technological resources. Overall [25] discovered that both people and government are contented by using SOA to achieve flexible and scalable E-government system. The author evaluated the e-readiness of Ethiopian people and endorsed SOA for loose-coupled, effective and reliable public service provision.

1.3 Relate Works

According to [26], security is one of the major downside of E-government system. Therefore, communications in the E-government system should be adequately protected. The author considered both technical and practical security challenges for E-government systems to propose critical success factors for E-government security. Also, [1] reviewed on security problems for management of security threats in E-government system. The author proposed an information centric networking (ICN) approach as a solution of E-government security challenge. This is to ensure that information both at rest and on-transit is adequately protected from tempering and disclosure. Ultimately, provision of security for E-government system is an important issue due to the rapid development of ICT and advancement in e-service provision.

E-government supports integration of e-service entities in an efficient, effective, accessible and transparent manner. Formulation of data protection enforcement at the design and architectural specification enables reliable E-government system. [27] identified adequate alignment of business logics with information technology (IT) capabilities as a vital approach of developing a trustworthy E-government initiative. [28] conducted a comprehensive review and identified security as one of the major requirements of E-government services. A study by [29] discovered that the development of SOSE-Based E-government is not yet matured in Southern Africa. Human-Computer user interface and business-IT alignment is some of the major areas that requires further attention. This study focus on the use of digital signature with RSA public key algorithm to achieve data integrity in SOSE-Based E-government system. Data integrity is one of the major CIA (Confidentiality, Integrity and Availability) security goals of any information system.

2. OBJECTIVES OF THE PAPER :

The objective of this study is to provide an end-to-end data integrity security protection for messages exchange across all intermediaries in SOSE-based E-government system by use of digital signature with RSA public key cryptography.

3. SECURITY CONCERNS :

Communications in SOSE systems between the client and server are effected at the message level. Therefore application level's security solution is necessary for data integrity to adequately protect SOSE-based E-government system.

(a) Generally, information security researchers are familiar with security provision for TCP/IP's client-server security mechanisms. Consequently, researchers focused on point-to-point security (see figure 2) instead of security of messages from message sender and its receiver across all intermediaries. Consequently, inappropriate security mechanisms are applied for the protection of SOA systems.

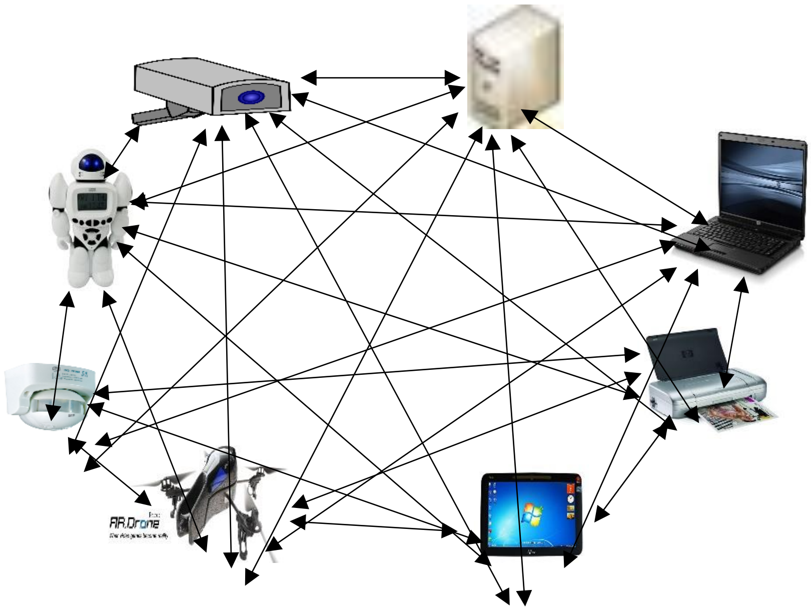

Fig. 2: Point to Point Connection of devices

(b) Usually interactions on the internet are designed by client-server connections on the transmission control protocol (TCP) to ensure accurate and reliable communications. With this protocol, an imaginary tube is created between client applications and server applications as shown in Figure 2. Therefore, to connect N applications in this protocol requires N(N-1)/2 number of connections (C). Consequently, to connect three and more applications (N>3), the number of connection will be greater than the number of applications (C>N) as shown in table 1. For instance, if the number applications is 10 (N=10), there will be 45 connections (C=45) and 20 applications requires 190 connections (C-190). The introduction of ESB mediator enables indirect connections between applications. This reduces the number of connections as shown in figure 3. Although as a result of this innovation, a new security problem arises.

Table 1: Characteristics of Point to point Connections

Node (N)	**No of Connection (C)** **= N(N-1)/2**	**Remarks**
2	1	Connection less than nodes (C<N)
3	3	Connection equal to nodes (C=N)
4	6	Connection greater than nodes (C>N)
5	10	Connection greater than nodes (C>N)
10	45	Connection greater than nodes (C>N)
20	190	Connection greater than nodes (C>N)

(c) The ESB enable interaction between sender and receiver applications with protocol. This protocol transformation by the ESB facilitates heterogeneous communication among applications with diverse protocols. This is different from the point-to-point communication of the traditional client/server distributed web applications. However, this requires reconsideration of security protection approach for SOSE systems.

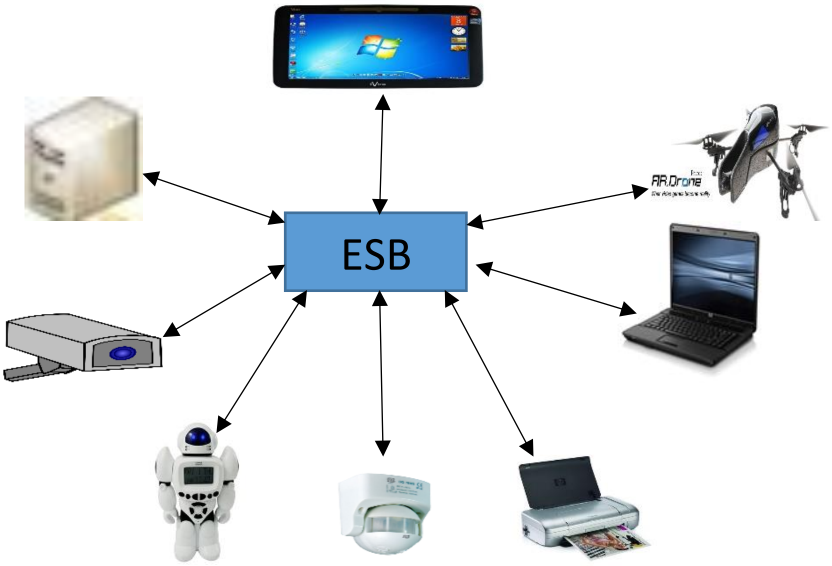

Fig. 3: SOSE Connection of Applications

Integrity is one the security goals of any information systems. Integrity solution for SOSE-based e-government should guarantee the accuracy and completeness all transmitted messages across the mediators. Active attacks are threats to the integrity of message, whereby the attacker manipulate messages' content unknown to both the sender and receiver of the message. The heterogeneous and dynamic nature of SOSE-based E-government systems renders it vulnerable to active attacks. Consequently, the integrity of the transmitted data is vulnerable due to the dynamic messages' transformation at the mediators. Since attackers can exploit the transmitted data while on transit either intentionally or unintentionally. Traditionally, messages in TCP client-server connections are vulnerable to active attacks as shown in Figure 4. There are two types of active attacks; message modification and replay attacks. Message modification attackers change part of the transmitted data while on transit unknown to both the sender and the receiver. While replay attackers intercept, replace and retransmitted the entire message to its destination unknown to both the sender and the receiver.

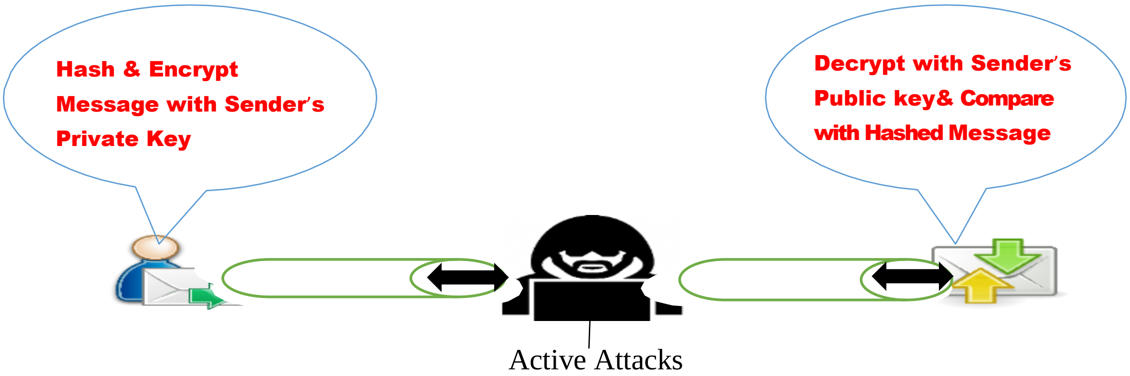
Hash & Encrypt Message with Sender's Private Key
Decrypt with Sender's Public key& Compare with Hashed Message
Active Attacks

Fig. 4: Integrity problem

[1] recommended that further studies be conducted on information security in E-government systems to its secure sensitive information on the network. Nowadays, development of E-government is gaining acceptance. Therefore, it is very important to investigate for strategies of improving security working toward security protected and reliable E-government systems. The focus of this study is to secure data movements in order to detect by verifying the validity of messages exchange from its origins to its destinations to protect government information. This study proposed use of public keys cryptography in conjunction with digital signature as an integrity solution for SOSE-government systems.

4. METHODOLOGY :

4.1 Justification for Use of Digital Signature with RSA Algorithm

The use of RSA digital signature for secret key exchange in this approach is highly efficient by the utilization of cryptographic hash function. The hash function reduced message of any length to a shorter value, called message digest, which satisfies two conditions. First, each message has a unique hash value. That is, no two digest can be hash from the same message. Second, no two messages can hashed to the same digest. The digest is the proof of the messages' integrity by verifying that the message representative are consistent at the signature verification operation. The message digest are to protect the integrity of the transmitted data by detecting any changes and/or alterations to any part of a message. In this approach, message digest are encrypted by RSA private key to create a digital signature.

The use of RSA digital signature offered several compelling benefits, particularly, use of RSA keys to achieve end-to-end security for SOSE system. The encryption of the message digest by RSA private key to obtain its digital signature avoids any changes to the message. At the verification process, the expectation is the decrypted digest of a digital signature to be the same compared with the hashed value digest. The choice of RSA digital signature for integrity in this approach is to ensure the preservation end-to-end SOA principles. Furthermore, this technique detects any slightest alteration made to the messages. This ensures accurate and consistent transmission of messages from its source to its destination across intermediaries.

4.2 Digital Signature with RSA

Amalgamation of digital signature with RSA public key refers to the use asymmetric key cryptography for signing and verification of signatures. The use of this approach need no key sharing, which is adequate for interaction in large open network. In this approach, the message sender hashes message to obtain the message's digest, encrypts the digest using private key of the sender to get the digital signature of the message. Subsequently, the sender transmits the original message and its signature to the receiver. At the receiver's end, the receiver gets the message and its signature. Therefore, the receiver hash functions the original message to get its digest and decrypts the signature of the message by the sender's public key to get another digest. Finally, the two digests are compared at the receivers end to evaluate if they are identical. If the two digests are identical proves that its integrity is intact and the message is authentic. The approach identifies any little change made in the message either by modification of the original message or replacement of the original message to reject it and ask for retransmission of the message. This approach detects both message modification and replay categories of active attacks.

Integrity is a security goal that is concerned with the accuracy and consistency of transmitted data. It ensures that unauthorized entities has no access as such only those authorized can modify transmitted data. However, avoiding access and modification to transmitted data is very challenging. Therefore, an approach to detect if tampering has occurred is crucial. Digital signature is designed to identify legitimacy of messages. This algorithms enables the receiver know the message's creator and it is untampered while on transit. Digital signature is an important algorithm used to enforce used to detect illegitimate messages on the network. This reveal the origin of all messages to the receiver as well as guarantees that the message is untampered while on transit and it is composed by a known sender. Digital signature algorithm transmits the signature attached to the document as an evidence that the document originated from the correct sender to the receiver.

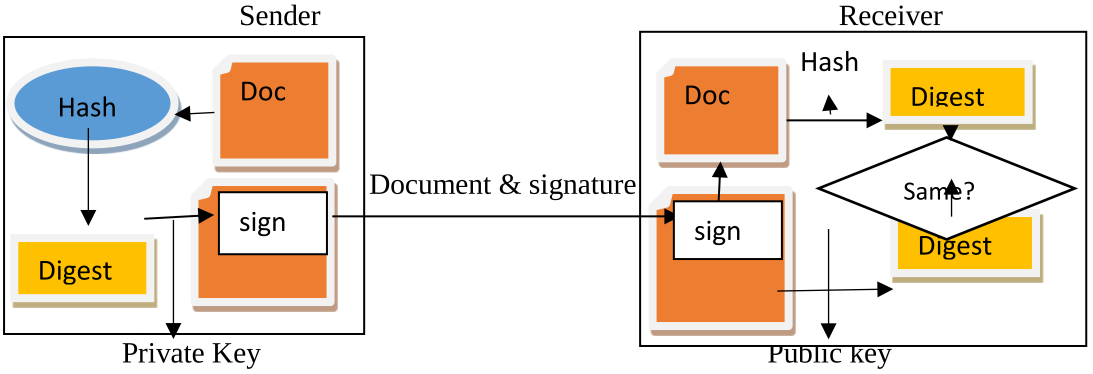

Fig. 5: Digital Signature with RSA

The procedures followed for digital signature with RSA shown in Figure 5 from the sender's side and the receiver's side is summarize below.

a. Sender's Side

i) The sender creates the message digest of the document through the hash algorithm,
ii) The sender encrypts the message digest using his/her private key to form the digital signature for the document,
iii) The sender appends the digital signature to the document and sends both the document and the digital signature to the receiver.

b. Receiver's Side

i) The receiver receives the document with the appended digital signature,
ii) The receiver separates the digital signature from the document,
iii) The receiver decrypts the digital signature to obtain the message digest,
iv) The receiver run the hash algorithm of the document to get its message digest,
v) Finally, the receiver compares the two-message digests, accept the message if the two digests is the same, and otherwise reject the message.

Finally, digital signature with RSA can ensure three security requirements, integrity, authentication and non-repudiation.

5. RESULTS AND DISCUSSION :

5.1 Experimental Results

This subsection presents the results of the study. Messages Exchange in SOA-based E-government systems are written in XML language enclosed in SOAP envelope. The SOAP envelope contains indicators of adequate digital signature with RSA to ensure data integrity.

Analysis of the messages' content revealed adequate formulation of digital Signature. Digital signature indicators were appropriately formulated. The message content shows that SignedInfo, SignatureValue and KeyInfo element were correctly formulated. The SignedInfo element in the SOAP message contains Canonicalization Method, Signature Method and Reference subelements. The outcome also shows that Signature Value element carries the encrypted message digest and the KeyInfo element carries the security token reference.

5.2 Advantages of the Security Solution

The use of RSA with Public key cryptography for data integrity has the following advantages:

i. It enables source-to-destination security of message across all mediators.
ii. It enhances flexibility and interoperability of the entire software system.
iii. It facilitates loose-coupling and agility of the application.
iv. It facilitates creation of many credentials suitable for large applications.

5.3 Disadvantages of the Security Solution

The security has the following disadvantages:

i. This solution does not support the implementation of data streaming over the network.
ii. It require sound understanding of XML security for adequate to implement the security solution
iii. It requires sound understanding of WS-security specifications, which is difficult to implement.

6. CONCLUSION :

Nowadays, the popularity of internet and ICT services globally improves online interactions among citizens, government and businesses. E-government system is the provision of online public services for transparency, efficiency, flexibility as well as enhanced quality of service delivery. However, maintenance of security is one of the major downside associated with E-government implementation. It is important to ensure that government network is adequately protected in view of the dynamic nature of security threats and risks. Integration of E-government with SOA provides agile, flexible, interoperable and autonomous services that communicates to support the operations of E-government systems. Although, this introduces new security issues that requires novel solutions. This paper uses digital signature with RSA algorithm to solve data integrity problem in E-government system.

REFERENCES :

[1] Priyambodo, T. K., Venant, U., Irawan, T., & Waas, D. V. (2017). A Comprehensive Review of e-Government Security. *Asian Journal of Information Technology*, *16*(2-5), 282-286.
Google Scholar↗

[2] Hassan, R. G., & Khalifa, O. O. (2016). E-Government-an Information Security Perspective. *International Journal of Computer Trends and Technology (IJCTT)*, *36*(1), 1-9.
Google Scholar↗

[3] Alsmadi, I., & Abu-Shanab, E. (2016). E-government website security concerns and citizens' adoption. *Electronic Government, an International Journal*, *12*(3), 243-255.
Google Scholar↗

[4] Sá, F., Rocha, Á., Gonçalves, J., & Cota, M. P. (2017). Model for the Quality of Local Government Online Services. *Telematics and Informatics*, *34*(5), 413-421.
Google Scholar↗

[5] Mosa, A., El-Bakry, H. M., Abd El-Razek, S. M., & Hasan, S. Q. (2016). A proposed E-government framework based on cloud service architecture. *International Journal of Electronics and Information Engineering*, *5*(2), 93-104.
Google Scholar↗

[6] El Benany, M. M., & El Beqqali, O. (2018, April). Choreography for interoperability in the e-Government applications. In *2018 International Conference on Intelligent Systems and Computer Vision (ISCV)* (IEEE, *18*(1), 1-4.
Google Scholar↗

[7] Yang, L., Elisa, N., & Eliot, N. (2019). Privacy and security aspects of E-government in smart cities. In *Smart cities cybersecurity and privacy*. Elsevier, *2019*(1), 89-102.
Google Scholar↗

[8] Sedeño, J., Salinas, C. J. T., Escalona, M. J., & Mejías, M. (2014, April). An Approach to Transform Public Administration into SOA-based Organizations. *WEBIST*, *1*(1), 135-142.
Google Scholar↗

[9] Almahmoud, A. A. (2020, September). E-Services Integration Framework Based on SOA. In *Proceedings of the 2020 12th International Conference on Information Management and Engineering*, *12(1)*, 1-6.
Google Scholar↗

[10] Kim, H. J., Lee, H. S., & Jung, Y. G. (2017). SOA-based Web Service Application and Analysis-forcused to Japan Electronic Government. *The Journal of the Convergence on Culture Technology*, *3*(1), 25-28.
Google Scholar↗

[11] Suzuki, T., & Suzuki, L. (2020). On the Benefit of 3-tier SOA Architecture Promoting Information Sharing Among TMS Systems and Brazilian E-Government Web Services: A CT-e Case Study. *13047*(1), 1-14.
Google Scholar↗

[12] Alghamdi, B., Potter, L. E., & Drew, S. (2016, June). Identifying Best Practices in organisational SOA Governance Adoption: Case Study of Saudi Arabia's E-Government Programme. In *PACIS 2016(1)*, 365-380.
Google Scholar↗

[13] Barakat, O., & El Beqqali, O. (2020, September). Business Intelligence and SOA Based Architecture for E-government System Interoperability. In *Proceedings of the 13th International Conference on Intelligent Systems: Theories and Applications*, *13*(1), 1-5.
Google Scholar↗

[14] El Benany, M. M., & El Beqqali, O. (2015, November). SOA based e-government interoperability. In *2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA)* IEEE, *12(1)*, 1-2).
Google Scholar↗

[15] Qusef, A., Ayasrah, A., & Shaout, A. (2021). Comprehensive Approach to Implement E-Government Backend in Jordan Using Service-Oriented Architecture. *International Journal of Software Innovation (IJSI)*, *9*(2), 122-135.
Google Scholar↗

[16] Jayawickrama, G. I. U. (2021). Customer Complaint Management System using SOA. University of Columbia digital library (Doctoral dissertation), *1*(1), 1-93.
Google Scholar↗

[17] Hodijah, A., Sundari, S., & Nugraha, A. C. (2018). Applying TOGAF for E-Government Implementation Based on Service Oriented Architecture Methodology Towards Good Government Governance. In Journal of Physics: Conference Series. IOP Publishing, *1013*(1), 1-8.
Google Scholar↗

[18] AlHajri, A., Al-Khanjari, Z., Kraiem, N., & Al, Y. Enhanced e-Government Integration Framework for Higher Interoperability in e-Government Initiatives. *2017 IEEE International Conference on Intelligent Computing, Instrumentation and Control Technologies*, *17(1), 1831-1846.*
Google Scholar↗

[19] Mesfin, G., Grønli, T. M., Ghinea, G., & Younas, M. (2017, August). Adopting SOA in public service provision. In *International Conference on Mobile Web and Information Systems* Springer, Cham, *2017*(1), 279-289.
Google Scholar↗

[20] Sofian, A. R. (2019, November). Designing SOA-based BATAN Public Services with Restful Web Service. In *2019 IEEE International Conference on ICT for Smart Society (ICISS)*, *7*(1), 1-6).
Google Scholar↗

[21] Sasono, D. S., Setyohadi, D. B., & Santoso, A. J. (2018). E-Government Integration Based on SOA for Supporting Sleman Smart Regency (A Case Study of Sleman Regency, Special Region of Yogyakarta). *ICCSET 2018, October 25-26, Kudus, Indonesia*, *1*(1), 360-366.
Google Scholar↗

[22] Fajar, A. N., & Shofi, I. M. (2019, August). Service Oriented Design for Indonesian E-Government System Using SOA. In *IOP Conference Series: Materials Science and Engineering*, *598*(1), 1-5.
Google Scholar↗

[23] Utama, A. P., Asmara, R., & Hasim, J. A. N. (2019). E-Government Integration of Sidoarjo Regency using Service Oriented Architecture (SOA). *IJNMT (International Journal of New Media Technology)*, *6*(2), 109-115.
Google Scholar↗

[24] Nakonechnyi, A., & Kolisnichenko, N. (2020). Service-Oriented Architecture of E-Government: Characteristics of the Anglo-American Model and Peculiarities of its Implementation in Ukraine. *Public administration and local government*, *47*(4), 39-48.
Google Scholar↗

[25] Mesfin, G., Grønli, T. M., Ghinea, G., & Younas, M. (2017). Adopting SOA in public service provision. In *International Conference on Mobile Web and Information Systems* Springer, Cham. *10486*(1), 279-289.
Google Scholar↗

[26] Shareef, S. M. (2016). Enhancing Security of Information in E-Government. *Journal of Emerging Trends in Computing and Information Sciences*, *7*(3), 139-146.
Google Scholar↗

[27] AlAbdali, H., AlBadawi, M., & Sarrab, M. (2019, November). Preserving privacy of integrated e-government information: Architecture approach. In *2019 2nd IEEE Middle East and North Africa COMMunications Conference (MENACOMM)* IEEE, *2*(1), 1-5.
Google Scholar↗

[28] Abraham, A., Hörandner, F., Zefferer, T., & Zwattendorfer, B. (2020). E-government in the public cloud: requirements and opportunities. *Electronic Government, an International Journal*, *16*(3), 260-280.
Google Scholar↗

[29] Ajibade, P., & Mutula, S. M. (2019). Bibliometric Analysis of Citation Trends and Publications on E-government in Southern African Countries: A Human-computer Interactions and IT Alignment Debate. *Library Philosophy & Practice*, *2156*(1), 1-19.
Google Scholar↗

****