# PENERAPAN KEAMANAN WEB-SERVICE MENGGUNAKAN METODE SOAP PADA PERANGKAT SMARTPHONE

**Sulvian Samudra[1)], Ansar[2)]**
[1]Sistem Informasi, STMIK Profesional Makassar
email: sulviands@gmail.com
[2]Sistem Informasi, STMIK Profesional Makassar
email: ansarroy5@gmail.com

***Abstract***

*The impact of the development of this mobile application resulted in the emergence of requirements regarding communication with other software components, especially related to security features. The process of adding security features to the transport layer provided by HTTPS may be sufficient for user applications, but does not meet the more sophisticated security requirements for large-scale enterprise applications. The gSOAP method is set up for the security plugin and the JNI adapter prepares the security configuration by leveraging the plugin. The security context adapter is configured from the Java class at runtime so the presence of OpenSSL allows the use of gSOAP security plugins to be applied on mobile platform devices. Provision of service authorization that has been determined in the username token header, while confidentiality is used in the data confidentiality process. XML Encryption is a versatile tool for encrypting XML documents in whole or in part. In order to securely present XML data, an XML flow is first created and arranged in a suitable representation so that unauthorized users cannot access the data. Through the application of XML format encryption, it supports more dynamic data communication between smartphone devices and maintains data security.*

***Kata Kunci** : Encrypt, xml, soap.*

## A. PENDAHULUAN

Peranan aplikasi yang saat ini sebagian besar digunakan pada perangkat seluler terutama untuk tujuan konsumen. Peningkatan jumlah aplikasi pada setiap perusahaan dapat menjadi sumber daya yang penting. Dampak dari berkembangnya aplikasi seluler ini mengakibatkan muncul persyaratan baru mengenai komunikasi dengan komponen perangkat lunak lain,terutama berkaitan dengan fitur keamanan.

Lingkungan perusahaan biasanya diatur berdasarkan proses bisnis yang mengintegrasikan banyak komponen sistem yang berbeda. Implementasi sistem perangkat lunak yang digabungkan secara kompleks dapat menghasilkan banyak layanan pada sistem. pada umumnya layanan berbasis web menggunakan metode SOAP karena SOAP adalah protokol standar dan platform independen yang memungkinkan fleksibel dan kaya fitur interface yang akan berguna dalam sebuah sistem . Pengguna akan mengkonsumsi layanan secara otomatis sehingga secara signifikan mengurangi beban kerja server ketika terjadi permintaan proses yang rutin dalam satu waktu.

Proses penambahan fitur keamanan pada lapisan transport yang disediakan oleh HTTPS mungkin cukup untuk aplikasi pengguna, tetapi tidak memenuhi persyaratan

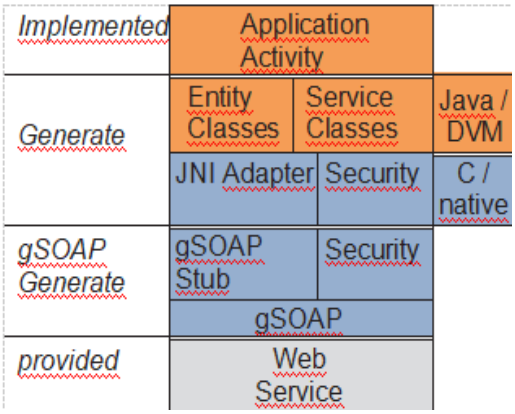
keamanan yang lebih canggih untuk aplikasi perusahaan berskala besar, oleh karena maka dibutuhkan web-service meggunakan metode SOAP berbasis REST dalam lingkungan perusahaan. Aplikasi perusahaan seluler sebaiknya mampu mendukung penerapan metode SOAP untuk memungkinkan integrasi dalam bisnis yang ada proses secara tepat, selain itu sebuah aplikasi ini harus dibuat mendukung otomatisasi menjadi lebih fleksibel pada perubahan interface yang kompleks dan untuk mempercepat proses pengembangan aplikasi, selain itu aspek keamanan juga berlaku untuk layanan web-service sehingga kualitas layanan dapat terjaga.

Berdasarkan latar belakang yang telah diuraikan maka penulis tertarik untuk melakukan penelitian dengan tema "**Penerapan Keamanan Web-Service Menggunakan Metode SOAP Pada Perangkat Smartphone**". Diharapkan penelitian ini dapat mendukung setiap perusahaan dalam meningkatkan dukungan layanan berbasis digital.

## B. METODE PENELITIAN

### 1. Konfigurasi Keamanan SOAP

Pada plugin keamanan menyediakan API untuk mengonfigurasi konteks keamanan layanan web metode gSOAP disiapkan untuk plugin keamanan dan JNI-Adapter menyiapkan konfigurasi keamanan dengan memanfaatkan plugin API. Dalam hal ini konfigurasi dikodekan dalam kode C dan selanjutnya menghasilkan library. Teknik lain yang dapat dilakukan yaitu mengenkapsulasi API plugin keamanan dengan JNI-Adapter konteks keamanan kemudian dikonfigurasi dari kelas Java pada pada saat runtime sehingga kehadiran OpenSSL memungkinkan penggunaan plugin keamanan gSOAP di aplikasikan pada perangkat platform mobile.




**Gambar 1.** Kerangka keamanan pada SOAP web service

### 2. XML Encryption pada SOAP

Enkripsi XML adalah alat serbaguna untuk mengenkripsi dokumen XML secara keseluruhan atau sebagian. Hasil terenkripsi akan dienkapsulasi pada tag XML penanda oleh Enkripsi XML. Kunci enkripsi, instruksi mekanisme yang digunakan untuk melakukan enkripsi, ciphertext, dan atribut lainnya didasarkan dalam elemen XML penanda. Tag Data Terenkripsi pada umumnya adalah elemen XML penanda berupa tag Encrypted Data.

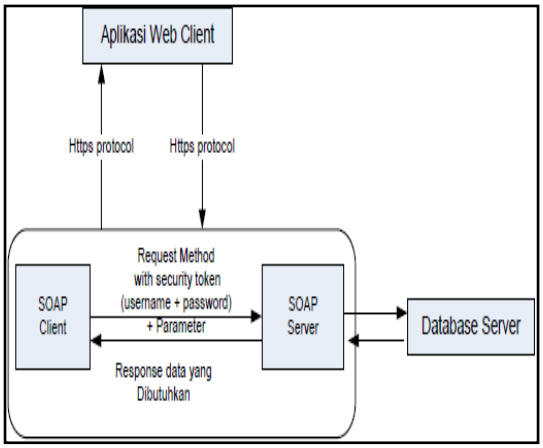
```
<EncryptedData Id? Type? MimeType?
Encoding?>
<EncryptionMethod/>?
<ds:KeyInfo>
<EncryptedKey>?
<AgreementMethod>?
<ds:KeyName>?
<ds:RetrievalMethod>?
                    <ds:*>?

</ds:KeyInfo>?
<CipherData>
<CipherValue>?
<CipherReference URI?>?
</CipherData>
<EncryptionProperties>?
                  </EncryptedData>
```

**Gambar 2.** Skema XML Encryption

## 3. Arsitektur Sistem

Sistem aplikasi yang akan dibangun memiliki arsitektur keamanan secara umum seperti pada gambar 1, di mana setiap request dari client akan dilakukan otentikasi, otorisasi, dan konfidensialitas. Otentikasi terjadi saat pengguna berhasil mengkses login serta diberikan akses ke sumber daya sesuai dengan hak aksesnya. Ketentuan pemberian otorisasi layanan yang telah ditentukan pada header username token, sedangkan konfidensialitas di gunakan pada proses kerahasiaan data.




**Gambar 3.** Mekanisme Otentikasi User pada SOAP

Metode penelitian menjelaskan rancangan kegiatan, ruang lingkup atau objek, bahan dan alat utama, tempat, teknik pengumpulan data, definisi operasional variable penelitian, dan teknik analisis. [Times New Roman, 12, normal].

## C. HASIL PENELITIAN DAN PEMBAHASAN

### Hasil Penelitian

### Penerapan WS-Security SOAP

Untuk menyajikan data XML dengan aman maka pertama-tama dibentuk alur XML dan diatur dalam representasi yang sesuai sehingga pengguna yang tidak sah tidak dapat mengakses data. Untuk menjamin kerahasiaan data, aliran data XML yang terorganisir harus dienkripsi sebelum di sajikan melalui saluran. Untuk mendukung pemrosesan quey XML pada pengguna perangkat mobile, beberapa informasi indeks harus diterapkan ke alur XML yang dihasilkan berdasarkan pada otorisasi akses yang ditentukan dalam dokumen XML asli.

```
Algorithm EncryptedXMLStreamGenerator
Input: A well formed XML Document;
Output: Encrypted XML Stream S;
1. contentHandler.startDocument(){
2. preorder = 1;
3. postorder = 1;
4. parentIndex = 0;
5. Stack secNodeStack = ;
6. secNodeList = ;
7. }
8. contentHandler.startElement(){
9. Construct a SecNode newSecNode;
10. newSecNode.setPreOrder(preorder);
11. newSecNode.setParentIndex(parentIndex);
12. if (parentIndex = 0){
13. newSecNode.setRootToNodePath("/"+tag name);
14. }else{
15. parentSecNode = Peek from secNodeStack;
```

**Gambar 4.** Algorithm pembentukan encrypted XML

```
16. newSecNode.setRootToNodePath(parentSecNode.getRootToNodePath()
+"/"+ tag name);
17. }//end If
18. if (the current element contains attributes){
19. for(int i =0; i < total number of attributes; i++){
20. Coustruct Attribute newAttribute;
21. newAttribute.setName(name of attribute);
22. newAttribute.setValue(value of attribute);
23. newSecNode.addAttribute(newAttribute);
24. }//end for
25. }//end If
26. Add newSecNode into secNodeList;
27. Push newSecNode into secNodeStack;
28. parentIndex = preorder;
29. preorder ++;
30. }
31. contentHandler.endElement(){
32. currentSecNode = Pop from secNodeStack;
33. parentIndex = currentSecNode.getParentIndex();
34. currentSecNode.setPostOrder(postorder);
35. postorder ++;
36. }
37. contentHandler.charachters(){
38. currentSecNode = Peek from secNodeStack;
39. currentSecNode.setText(content of element);
40. }
41. contentHandler.endDocument(){
42. for(int i = 0; i < secNodeList.length(); i++){
43. Find the field Min (NCS) for secNodeList.get(i);
44. Find the field Min (NIS) for secNodeList.get(i);
45. }//end for
46. Construct the encrypted XML stream S from the secNodeList;
47. }
```

**Gambar 5.** Algorithm pembentukan encrypted XML

**Proses Query XML Encrypted**

Di bagian ini dijelaskan bagaimana pengguna perangkat smartphone dapat memproses berbagai jenis quey XML melalui alur XML terenkripsi menggunakan struktur SecNode. Untuk memproses query XML melalui aliran XML terenkripsi, maka dibangun algoritma proses query xml terenkripsi untuk digunakan secara dinamis.

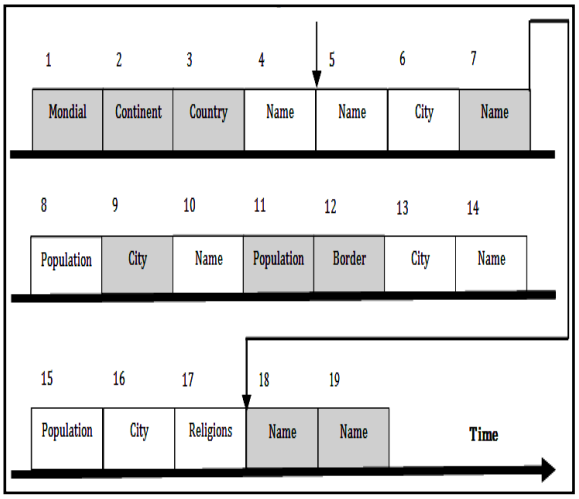
```
Algorithm proses query xml terenkripsi
Input: Encrypted XML Stream S, XML Query Q, List of Keys K;
1. R = ;
2. flag = false;
3. while (stream S has not ended){
4. Read SecNode one after another until a SecNode appears on the air
encrypted with a key which is in K;
5. decSecNode    Decrypt SecNode;
6. If(depth(decSecNode.getRootToNodePath())== depth(Q)){
```

**Gambar 6.** Algorithm Query XML Encrypted

```
7. If(decSecNode.getRootToNodePath()==Path of Q){
8. If(decSecNode satisfies Predicate Condition of Q){
9. Insert decSecNode into R;
10. }//end If
11. If(decSecNode.getMinimalofNCS() != null){
12. Wait in doze mode until the target node arrives on the air;
13. }else{
14. break;
15. }//end If
16. }else{
17. If(parentPath(decSecNode.getRootToNodePath())!= parentPath(Path
of Q)) && (decSecNode.getMinimalofNIS() != null){
18. Wait in doze mode until the target node arrives on the air;
19. }else{
20. break;
21. }//end If 22. }//end If 23. }end If 24. }//end while 25. return R;
```

**Gambar 7.** Algorithm Query XML Encrypted

Contoh pemrosesan queri jalur sederhana melalui aliran XML terenkripsi menggunakan bidang ( ) diilustrasikan dalam sebagai berikut :




**Gambar 8.** Alur query XML Encrypted

Jika pengguna seluler tidak dapat mendekripsi node 5 maka klien seluler terus melakukan permintaan untuk proses dekripsi. Saat node 7 dalam status tidak digunakan maka klien mendekripsinya node 7. Setelah mendekripsi node 7, perangkat webservice pada peranfkat smartphone akan menghitung kedalaman node 7, langkah selanjutnya adalah Mobile client menemukan bahwa kedalaman node 7 sama dengan kedalaman query XML, sehingga status node 5 diterima untuk melakukan eksekusi node 7 terhadap hasil dari Queri XML pada webservice. Tahap akhir yang dijalankan adalah data hasil query ditampung dalam antrian hasil dekripsi pada node 18.

ng berekstensi .jpg atau .png dan harus dimasukkan ke dalam text, sebagai contoh lihat **Gambar 1.** Keterangan gambar diposisikan dibawah gambar menggunakan nomor berurutan dituliskan menggunakan Times New Roman 10pt.

## D. KESIMPULAN DAN SARAN

### 1. Kesimpulan

Kesimpulan yang diperoleh dalam penelitian ini adalah Kemanan webservice dapat diterapkan pada metode SOAP melalui teknik enkripsi menggunakan format XML. Melalui penerapan enkripsi format XML mendukung terjadi nya komunikasi data antara perangkat smartphone yang lebih dinamis serta dapat menjaga keamanan data.

### 2. Saran

Untuk menghasilkan aplikasi yang lebih baik, penulis menganjurkan menggabungkan metode SOAP dengan plugin yang dapat mendukung percepatan pengiriman data dan mempertimbangkan untuk membangun algoritma untuk dapat diterapkan pada bahasa pemrograman yang lebih ringan seperti Python.

## DAFTAR PUSTAKA

[1] **Haviluddin Haviluddin(2019),** A Database Integrated System Based on SOAP Web Service**,** Association for Scientific Computing Electronics and Engineering (ASCEE), Indonesia Section, Indonesia, 2019.

[2] **Nandang Hermanto(2017)**, MODEL INTEROPERABILITAS ANTARA SISTEM AKADEMIK DAN SISTEM PERPUSTAKAAN MENGGUNAKAN WEB SERVICES,ISSN : 1979 – 925X e-ISSN : 2442 - 4528, Jurnal Telematika Vol. 10 No. 1 Februari 2017.

[3] **Ari Muzakkir(2012),** Rancang Bangun Keamanan Web Service Dengan Metode Ws-Secuirty, IJCCS(Indonesia Journal of Computing and Cybernatics System) (2012).

[4] **Ari Muzakkir(2013),** Perancangan dan ujicoba sistem keamanan web-service dengan metode WS-Security , jurnal ilmiah MATRIK Vol.15. No.1, April 2013 01-10.

[5] **R. Hidayat(2013),** Penerapan metode WEB service untuk integrasi layanan Puskesmas dan Rumah sakit, berkala MIPA,(23)1, Januari 2013.

[6] **Ari Muzakkir(2013),** SISTEM KEAMANAN DATA PADA WEB SERVICE MENGGUNAKAN XML ENCRYPTION, Seminar Nasional Teknologi Informasi dan Multimedia 2013.

[7] **Hartati Deviana(2011),** Penerapan XML Web service Pada Sistem Distribusi Barang, Jurnal Generic, Vol. 6, No.2, Juli 2011, pp.61~70 ISSN: 1907-4093.

[8] **Luc Bouganim(2011),** Philippe Pucheral. Dinamic acces-control policies on XML encrypted data. ACM Transactions on Information and System Security, Association for Computing Machinery, 2008, 10 (4), pp. 1-37.

[9] **Widodo S(2012),** Sistem Keamanan Transaksi Data Dengan Menerapkan Xml Enkripsi dan XML Signature Dengan Menggunakan Metode fast, Seminar Nasional Aplikasi Teknologi Informasi(2012).

[10] **Putra M(2019),** ANALISIS PERBANDINGAN METODE SOAP DAN REST YANG DIGUNAKAN PADA FRAMEWORK FLASK UNTUK MEMBANGUN WEB SERVICE, Jurnal Teknologi Informasi dan Komunikasi(2019).

[11] **E. Martins(2014),** Security testing methodology for vilnerabilities detection of XSS in web service and WS-security, Electronic Notes in Theoretical Computer Science(2014).

[12] **Matjaz B(2006),** Comparison of performance of Web service, WS-Security,RMI, and RMI-SSL, journal of System and Software(2006).