CHAPTER 2
LITERATURE REVIEW

In the past, many research works have been carried out on XML security and access control to the XML documents. This chapter provides a survey of the related work in these areas.

2.1 XML SECURITY


Schadow (2005) explained the use of the XML-Security Plug-In for Eclipse and CrypTool, which allow the users to apply XML encryption and signature to XML documents effectively. Schrefl et al (2005) presented a security method to ensure the privacy of documents, which are stored in the server after client side encryption.

Lee & Whang (2006) proposed a new Query Aware Decryption algorithm for the effective processing of XML queries against encrypted XML data. Their algorithm allows the users to decrypt not only the parts of
the query results but also full query results. Moreover, they used an XML index along with the encrypted XML data for enhancing the processing performance since this index helps to specify the location of the query results in the encrypted XML data. Yang et al (2006) proposed a Queriable XML Encryption (XQEnc) method, which is a new XML encryption technique, based on XML vectorization and used skeleton compression techniques. Their system computes compressed skeleton and a set of data vectors, which are encrypted separately. It also includes SAML and XACML.

Vasudevan & Yang (2006) proposed a rule-based security engine that is capable for enforcing security policies by enhancing the Apache Axis. By using this engine, it is possible for the developers of web services to declare the necessary security attributes for securing their applications. The main advantage of their approach is that, it allows reusing the security engine for different web services. Weerasinghe et al (2006) presented an XML encryption and signature algorithm based on mobile web services environment for health care application to protect data against malicious users.

Ardagna et al (2007) presented about XML signature and encryption, for providing security to XML databases. Moreover, they explained XKMS, which provides the registration, location, and validation techniques for public keys, used together with XML signature and encryption. They also presented two XML-based access control languages, namely, XACML and WS-Policy. Kato et al (2007) applied XML signature and encryption to provide authentication, data confidentiality, and integrity in a peer-to-peer platform. Kangasharju (2007) presented an XML encryption and signature technique, which can be used in mobile devices to provide security to mobile devices. Yixiang et al (2007) explained about information leakage while publishing XML documents and they proposed a new algorithm, called
Eliminate Inner Nodes (EIN) algorithm, in order to protect the sensitive data. Moreover, their algorithm is capable for retrieving a partial document from an XML document securely without causing information leakage.

Chang & Hwang (2007) proposed a new language, called Document Security Language (DSL), which supports the operational model of the document security system. Qiao (2007) demonstrated that the XML united signature structure could resolve the authenticity, integrity and non-repudiation problems of the data in the multi-operation chain, based on the XML communication. In their work, the <UnitedSignature> is the root element of the XML united signature, and it contains three elements, namely, <SubDigests>, <Signature>, and <UnitedSignatureObject>. Cho (2007) proposed an integration between XML encryption and access control to achieve the security requirements in the level of transport layer and in the access of different users.

Hai-hua et al (2008) proposed a new digital signature technology, since the existing signature schemas are not sufficient to handle the new XML requirements of a fine-grained signature and multiple signatures. Their proposed multi-signature scheme is based on the Ron Rivest, Adi Shamir, and Leonard Adleman (RSA) signature algorithm. Their model uses the XPath transform rules of the XML correlation techniques to divide the documents into sub-documents. In this schema, the owner digitally signs each sub-document, which can be verified by the receiving entities. Kundu & Bertino (2008) proposed a new approach for content dissemination, which has the structural properties of the XML DOM. Their approach provides an efficient dissemination and assures both content integrity and confidentiality. This is due to the fact that, it based on the encrypted postorder numbers, which supports the integrity and confidentiality requirements of XML content. Chang & Hwang (2008) proposed a new XML query language,
called the secure XML Query (sXQuery) language with an editor based on the XQuery language. sXQuery provides the features of both XQuery and DSL languages.

U’ñay & Gu’ndem (2008) presented a survey on indexes used for querying the encrypted XML documents. Their survey explained two types of indexes, namely, structural and value indexes and presented the various techniques used in indexing at both client side and server side. The structural index determines whether the path in the XML query matches with any of the paths in the XML documents. The value index checks the constraints provided in the range queries. Moreover, it lists the possible attack types and the cryptanalysis techniques to be used for encrypted XML documents. Sun & Li (2008) explained about XML and web services security standards in their paper. The XML security standards include the XML digital signature and encryption.

Gao et al (2008) proposed the XFlat technique for access control to XML documents. This technique is more concerned on query performance on the published XML view and thus protects the sensitive data using encryption techniques. By using an XML index tree, Xi-quan et al (2008) proposed a transformation-based algorithm for the retrieved of information based on semantic path. Their proposed algorithm is useful to the users to find subtle granular and helps in significant information to be signed quickly. Though their proposed algorithm enhanced the efficiency of XML multi-signature, it did not affect the data security. Brechlerova & Candik (2008) demonstrated the technologies of XML security and described their benefits in health documentation.

used for implementing the dynamic data handling on a web browser. Hashizume & Fernandez (2009) presented two patterns, namely, a Symmetric Encryption pattern to describe the basic type of algorithms and the other pattern is the XML Encryption, which describes a method of applying symmetric and asymmetric encryption techniques to XML messages. Knap & Mlýnková (2009a) analyzed the current security challenges in the XML signature and presented the suitable solutions.

Nordbotten (2009) presented about the XML security standards and web services. The XML security standards include XML signature, XML encryption, XACML, SAML, and XKMS. The web services include WS-Security, WS-Trust, WS-SecureConversation, Web Services Policy, and WS-SecurityPolicy. Jensen et al (2009) presented about XML namespaces in the domain of XML signatures since it has critical deficiencies, which can lead to vulnerabilities through XML signature wrapping attacks. Moreover, they described the problem of namespace injection and showed an attack scenario based on this technique. Moreover, they discussed several new approaches to overcome this threat.

Doroodchi et al (2009) presented about the service security based on XML and the various forms of XML-based attacks. Moreover, they provided recommendations and countermeasures for the attacks. Ping & Laihong (2009) presented a new approach on how to use the XML encryption and signature for effective logistics data exchange. Elgedawy et al (2009) proposed a new query-aware approach for compressing and encrypting large XML documents, while maintaining queriability over the intermediate document. Their proposed approach separates the document structure from its contents using the Ctree+ XML indexing approach. In addition to the separation, it applies context-free lossless encryption and compression techniques over the Ctree+ intermediate representations. Knap & Mlýnková (2009b) presented different processing approaches to the process of
verification of the web services integrity. Rahaman et al (2009) proposed an ontology-based XML content distribution system to protect the document content from unauthorized users and to protect the document structure form other organizations.

Xuan-min et al (2010) proposed to retrieve the encrypted XML data, using value and structure indexes, and discussed about the bucket management of the entrance addresses. Ammari & Lu (2010) proposed a new architecture to handle bulk XML messages, which has the ability to encrypt the sensitive parts of each message effectively using different types of encryption. Jie (2010) proposed an algorithm for XML document information management, based on equal element method. Their algorithm is capable of transforming a secret message into a decimal integer and creates an equal element by applying permutations and combinations to sub-elements. It inserts an integer into the XML document by exchanging some elements with their equal element based on a mapping function defined from the equal element to the integer. Jing (2010) analyzed about security system and the role of the XML technology in the security significance.

Zhihong & Yu (2010) presented a new system in university information platform. The system uses XML encryption and signature algorithm. They considered authentication, confidentiality, and integrity, while performing transfer and storage of the data. Yan & Xiuping (2010) proposed a system using XML encryption to provide a secure transmission of electronic records pertaining to medical applications. Chen et al (2010) presented a model with grammar structure, implementation, and its application for security based on XML digital signature.

Al-Hamdani (2010) proposed the use of XML for security implementation in their web-based healthcare applications. Luo et al (2010) implemented the Attribute Based Encryption (ABE) technique in web
services. Their technique aims to provide effective security and privacy preservation mechanism in web databases, instead of using XML encryption and XACML. Almarimi & Alsahdi (2010) proposed a cryptosystem for the encryption as well as the decryption of XML documents using a hybrid of RSA and Shift cipher algorithms. Their system improves the security by enhancing confidentiality, authentication, integrity, and non-repudiation. Haron et al (2010) proposed a Document Management System (DMS) for a web environment based on C/C++. Their DMS system generates secure documents using the XML encryption. The XML signature is used in their work for signing the documents before sending them to the intended recipients.

Somorovsky et al (2010) proposed a streaming-based Web Services Security Gateway (WeSSeGa) in SOAP messages. They provided a comparison between WeSSeGa and Java XML Digital Signature API. From their experimented works, they showed that, the streaming-based approach provides more performance improvements with respect to memory consumption and the evaluation time. Chen-xi et al (2010), based on the conic over the ring Z\textsubscript{n}, proposed an improved ElGamal digital signature scheme, named CCC-i-ElGamal, which achieves more security than the original ElGamal schema. Juan & De-ting (2010) proposed an enhanced query-processing algorithm for encrypted XML data, using hash tables and chained lists to create the indexes for user keys. Their algorithm permits users to decrypt only the needed parts to the query result. Moreover, their algorithm disseminates an encrypted XML index with the encrypted XML data. Yue-sheng et al (2010) presented an overview about the XML signature and encryption technologies and described the steps of applying the XML signature and encryption.
Hao-yu et al (2011) proposed a new encryption model by combining symmetric key and public key encryption technologies to provide a shared symmetric key distribution algorithm. In their model, the symmetric key is used to encrypt the sensitive data, and the public key is used to encrypt the symmetric key in order to ensure the security in data transmission. In their model, the receiver has to use his private key to decrypt the symmetric key. This symmetric key can be used to decrypt the encrypted data. Similarly, the sender uses his private key to verify the identity of the sender and to maintain data integrity. Ladan (2011) classified the new levels of threats in his paper into service level and message level threats. In each class, the author described many threats and discussed about the existing mechanisms to handle them. Onashoga & Sodiya (2011) proposed a security system on an examination application, which transfers the examination results in a secure way. They have adopted the XML encryption and signatures to ensure the security goals, namely, confidentiality, integrity, authenticity, and non-reputability, while exchanging electronic results.

Chang & Hwang (2011) proposed a query-processing model for processing the encrypted XML documents, using the XQuery language effectively. Their model translates automatically the XQuery statements for the encrypted XML documents by applying DSL rules to encrypt the XML documents and Schemas, based on the original XML documents. Xiang & Wang (2011) proposed an asymmetrical encryption algorithm, called XRSA, based on XML. It is a combination between the asymmetrical encryption algorithm RSA and an XML encrypter device. Liu & Chen (2011) described a prototype of XML security for a certificate management and presented the design and implementation of the XML signature and encryption. Jensen & Meyer (2011) described the techniques of attackers to intrude to web services communication even in the presence of the XML signatures and described the interrelation between the XML signatures and encryption. Ammari et al
(2011) proposed a new model to act as an Intelligent XML tag classification model for the XML encryption. Their model proposed mainly to improve the security and efficiency of an XML messaging system. Their model uses on-the-fly mechanism for classifying XML messages, creating three layers, and applying fuzzy logic approach to determine which parts of the XML message needed to be secured depending on importance level attribute.

Seak & Siong (2011) demonstrated that, the applying of the XML encryption and decryption to any binary document would not change the integrity of it. Jager & Somorovsky (2011) proposed an attack model to enable an intruder to decrypt arbitrary data that are encrypted according to the XML encryption, based on a cryptographic weakness of the Cipher Block Chaining (CBC) mode. Fu & Wei (2011) proposed a sequential multi-signature scheme through a middleware technology to implement it in the electronic document system to sign and verify the HTML documents. Song & Cui (2011) proposed an electronic voting scheme of signature based on the ElGamal blind-signature algorithm. Their program has the ability to solve voters' fraud in thee-voting and to prevent multiple votes from the same voter. Pin-ai & Xiang (2011) analyzed XML security and described an approach on how to apply the XML security technology to the practical integrated circuit card system, to provide confidentiality, integrity, authenticity, and non-repudiation of the campus smart card system.

Li & You (2012) represented the log of typesetting on the web, as an XML document, and applied the XML signature technology to protect it. In their work, the .NET Framework is used for implementing the XML digital signature and validation of the log of typesetting on the web, using C# programming language. Mahfoud & Imine (2012) proposed an approach to handle query recursive XML views in a secure way using only the expressive power of the standard XPath. Geric & Vidacic (2012) presented the Information system architecture and the implementation of a web service.
They explained the difference between the XML digital signature and standard digital signature. Somorovsky & Schwenk (2012) analyzed the countermeasures against the new chosen-ciphertext attack on the XML encryption proposed in Jager & Somorovsky (2011), and they showed the reasons on why the countermeasures cannot handle this attack. Moreover, they have proposed two practical countermeasures against it. Wu et al (2012) proposed a technique for the analysis of the OpenXML based Office series encryption mechanism. Quevedo-torrero & Erickson (2012) presented a querying implementation of XML. Their framework exploited the Prolog based data structures leading to the handling of deductive and recursive queries.

Liu & Chen (2012a) proposed a method to transform XPath to XML data, using a hashing technique to provide effective integrity checking for decomposed XML data. They provided a signer to check the integrity without cooperation from other signers. Liu & Chen (2012b) proposed a number list based interval-labeling scheme for XML data encryption. When there is no space available for node insertion, the schema assigns a number for the sub-tree to be inserted, and performs a new labeling process for each node in the sub-tree. The main advantage of their model is its ability to handle updates effectively. Nithin & Bongale (2012) proposed a new public key cryptographic algorithm, named XML Batch Multi-Prime RSA (XBMRSA) to encrypt the XML documents. Their algorithm is based on Multi-Prime RSA technique. The main idea is using multiple of prime numbers to compute the modulus for both the public and private keys (N), instead of two prime numbers as in the standard RSA. Their techniques needs less computation time for the encryption of the XML documents, and it is more efficient public key cryptographic algorithm than the Standard RSA algorithm. Algarin et al (2012) presented a new UML class diagram, called an XML Schema Class Diagram (XSCD) to transition an XML schema into an UML schema.
Moreover, they defined a new UML XML Role Slice Diagram (XRSD) that allows permissions to be defined against XML schema elements in the XSCD. Finally, they transited these XSCDs into a corresponding security policy to generate automatically an XACML policy for enforcement of the XML schema at the instance level. Li-yan & Huan (2012) proposed a design and realization of electronic commerce platform based on the XML signature.

Cao et al (2013) proposed an efficient evaluation of tree pattern queries on the encrypted XML documents. They embedded each XML document in a hierarchy and created a vector, which encoded the information about each XML document. Moreover, they created a vector for tree pattern queries and matched between the two encrypted vectors.

2.2 ACCESS CONTROL TO XML DOCUMENTS

Tan et al (2001) proposed an algorithm, called XML sEcurity eNforcement Architecture (XENA). XENA is an access control system for XML documents stored in relational database. The XENA maps XML documents in relational tables and uses authorization rules to designate the information that must be protected. Moreover, XENA verifies the retrieved information against the authorization rules to filter the protected information. XENA conducts to the access control rules from outside the relational engine, which leads to a performance overhead.

Murata et al (2003) proposed a static analysis model for XML access control. However, their technique increases the time complexity, while checking the security of queries when static analysis fails. Fan et al (2004) proposed a complex and an expensive technique to express access control policies using XPath queries. Wu et al (2005) proposed a new Authorization Policy Sheet (APS) tool to describe the authorization rules for the XML documents. Moreover, the Document Type Definition (DTD) is used to
translate the rules described in an APS into a standard XML document. Kuper et al (2005) proposed a generalization of XML security views. Their model specifies the policies over DTDs with XPath expressions. Mohan et al (2005) proposed a technique for security views. Their technique is restricted on hiding node values.

Fan et al (2006a) proposed an XML security framework to protect sensitive data from direct access or indirect inference through queries by unauthorized users. Their framework supports fine-grained access policies according to the structure and values of the protected XML data. Moreover, their framework assists the security administrators to derive views specification automatically. Finally, their framework provides a view schema to different user roles, which makes it possible to guide users when they are running queries on the system. Fan et al (2006b) proposed a Secure MOdular Query Engine (SMOQE) approach to rewrite, evaluate, and optimize queries on XML views. Lv & Yan (2006) proposed a framework web, called Web Application Level Security Gateway (WALSG) to provide web security. Their framework is based on the two proposed languages, namely, Access Control Policy Description Language (ACPDL) and Security Policy Description Language (SPDL). Their framework is capable for securing the existing web sites and creating new web sites in a secure way.

Ganesan & Mohamed Jamal (2006) proposed an integration approach between the bitmap based access control approach and cryptography. Their integration allows to the generation of the ePath level access control, using two dimensional access control matrix, instead of using three dimensional security cubes. Therefore, their approach saves the redundant storage space needed at the server for storing the restricted views of the XML documents. Sanchez et al (2006) proposed a simple approach to the XACML policies specification, based on the use of high-level templates and
Infopath application. An XACML policy is generated automatically, using an XML transformation as the templates that are built from XML schemas. However, they neither provided any details about the methodology nor the practical implementation of their approach. Anderson (2006) presented a comparison between the policy language, namely, Enterprise Privacy Authorization Language (EPAL) and XACML. The two languages have been developed for expressing the privacy policies. The conclusion of the comparison ensures that, the functionality of XACML is more powerful than EPAL.

Fu & Ye (2007) proposed an access control model, based on the users' and roles' attributes. Their model uses users' and roles' attributes as part of the access control policy. Moreover, they proposed an XACML-based policy language, namely, A-XACML based on XACML. Ro’der et al (2007) proposed a model for access control to the XML documents, based on the current document content and history information that recorded the operations performed on that document. Chang et al (2007) solved the limit of Mohan et al (2005) by considering constraints based on structural relationships between elements.

Kim et al (2008) proposed an algorithm to store the XML data and XML access control rules in a relational database. Their algorithm allows users to exploit the features of relational database systems, to check the security of the XML documents, and run queries on them. Lang et al (2008) proposed an XACML policy generating method, based on a user-oriented ABAC policy view. Moreover, they proposed a new ABAC concept model, called Access Control Cube (ACCube) and presented a policy description template composed of primary policy description elements of XACML. Khurat & Abendroth (2008) proposed a mechanism where the Policy
Decision Point (PDP) evaluates the request only once when multiple resources are requested, hence, the processing time is reduced.

Scaglioso et al (2008) presented a complete description of XACML and the implementations of the basic XACML components. In addition to the description, they listed the XACML benefits, drawbacks, and open issues to improve XACML. Sasaki et al (2008) proposed a fine-grained access control model, based on logic programming in hybrid relational XML database. Their model is capable for restricting the access to the relational and XML data. For the relational data, the restriction is applied at the cell-level. However, it is applied at the node-level for the XML data in a cell. Li et al (2008) proposed an approach to find the defects of the XACML implementations. Their approach determines the defects by testing the behaviors of different XACML implementations for the same XACML policies and requests, and observing whether the different XACML implementations produce different responses or not.

Peng et al (2008) proposed an approach to match dynamically the semantics of the users and information in the XML documents to control the access to them. Rahaman et al (2008) proposed a distributed and fine-grained access control mechanism, based on the encryption for the XML documents. The proposed technique achieves the confidentiality, authenticity, and integrity. Karusseit et al (2008) presented a comparison between XACML and WS-Policy with the constraints and graph-based approach for modeling access control. Duong & Zhang (2008) proposed a fine-grained access control model, namely, SecureX to query and update XML data securely. Their model allows users to read and write, and it is capable for defining rules explicitly for the users to authorize the access to XML data. Li & Hong (2008) proposed an extension to the authorization term to be AUTH (Authᵣ, Authᵣᵩᵣ). Their extension presents the time information in the authorization
rules. Moreover, they proposed a bitmap indexing technique with time information and proposed an authorization-processing algorithm, to retrieve the correct authorization decision.

Bouganim et al (2008) proposed a streaming evaluator of access control rules, to provide a powerful fragment of the XPath language. They designed a streaming index structure allowing overtaking the unauthorized parts of the input document. They proposed a technique for the management of pending predicates compatible with a streaming delivery of the authorized parts of the document. They proposed a secure mechanism to refresh the SOE access control rules from a potentially malicious server. Moreover, they proposed a combination of hashing and encryption techniques to ensure the integrity of the document. Mazzoleni et al (2008) proposed an integrating algorithm, to integrate two well-formed XACML policies. Mohy & El-Sharkawi (2008) proposed an approach, namely, Disclosure Prevention Algorithm (DPA). Their approach combines the role based access control models with the power of inference engine, to prevent unauthorized users from inferring critical information.

Qu et al (2009) discussed about the access control and security specifications, defined on DTD with production expression, and explained how to construct security XML views. Laborde et al (2009) extended the XACML authorization web service by adding a core element to it that implemented both XACML and additional modules, for providing new security features for securing information. Their extension is applied to dynamic web sites access control management. Hsieh et al (2009) proposed an extension to the XACML policy language by adding a <ResourceContent> within a <Resource>. Aburahma & Stumptner (2009) proposed a Spatial Role-Based Access Control (SRBAC) model, using XACML. Their model is an extension of RBAC to combine location information in access control decisions. Ardagna et al (2009) proposed a privacy-aware access control
system. Their system is implemented in PrimeLife project and is compatible with XACML. Koromilas et al (2009) proposed a re-annotation algorithm to control the access to the XML documents stored in relational and native XML databases. While the update operation, their algorithm runs the XPath query, that retrieves the XML nodes to be re-annotated.

Lischka et al (2009) proposed the concept of deductive policies in XACML that permit to specify policies on the Software as a Service (SaaS) service. Their deductive policies help to deduce the decision. Mondal & Sural (2009) proposed an XML based policy specification framework, namely, Enhanced Spatio-Temporal Role Based Access Control (ESTARBAC) for spatio-temporal RBAC model. Their framework describes the spatio-temporal extent. This extent provides a variety of spatio-temporal access control policies, such as role hierarchy, separation of duty, and cardinality. Ferrini & Bertino (2009) proposed a new framework by integrating XACML and Web Ontology Language (OWL) frameworks. Therefore, it provides the features of both OWL ontologies and XACML policies, for supporting RBAC. OWL handles the role hierarchy and constraints and XACML handles the authorization policies.

Dai et al (2010) proposed the architecture of Usage Control (UCON) model in web services and explained access control models and XACML. Jing et al (2010) provided a description for a general security policy, namely, XML-Based General Policy Description (XBGPD). They defined the behavior of the system’s entities. Moreover, they discussed the logic relationship in policy’s element and showed XML-based description rules about the policy. Landberg et al (2010) proposed a novel privacy-aware access control model for XML. Their model uses the query-time access control for combined access to nodes. Moreover, they proposed a security level composition to group nodes in the XML data. Abassi et al (2010) made a comparison between XACML policies and
annotated schemas and identified the significant fragment of XACML. Moreover, they proposed translation algorithms from XACML policies into annotated schemas.

Jinsong et al (2010) proposed an access control model, based on RBAC to handle the access of the users to the resources and authorize the users' rights. Their model is implemented in the XML documents for complex business process using J2EE. Hsieh et al (2010) proposed a combination of XACML, XML encryption, and XML digital signature, to provide a secure, embedded, and fine-grained access control policy. Their combination allows for embedding the content to be protected with the access control policy statements in the same XACML document. In their model, the content is protected by the XML encryption for confidentiality and by the XML digital signature for authentication and integrity. Arunkumar & Rajarajan (2010) proposed an architecture to access control the data privacy through mobile devices, using XACML policy. Alm & Illig (2010) proposed a translation approach from ORKA Policy Language (OPL) into XACML. In their approach, the administration of high-level access control concepts and the authorization constraints are combined together with XACML. The aim of their approach is to solve the problem of the XACML policies administration.

Rota et al (2010) proposed an approach to combine between the advantages of the XACML policy language and OWL. Moreover, they proposed a practical privacy filtering application to filter out the required information from the XML documents with respect to a set of XACML semantic privacy policies. Bekara et al (2010) proposed a privacy aware XPACML policy language model to combine the advantages of XACML and Platform for Privacy Preferences Project (P3P). Their model allows the users and service providers to define their privacy and policies in XACML format. Chou & Huang (2010) proposed an extended XACML model, namely,
EXACML to provide more secure information access to web services. Their model is an extension of XACML and based on the concepts of information flow control to avoid the leakage of information. Helil & Rahman (2010a) tried to solve the XACML complexity by proposing an extended XACML profile for RBAC by using an OWL base approach. Helil & Rahman (2010b) proposed an extension to the XACML profile for RBAC to provide constraints, such as static and dynamic separation of duty and role cardinality. Moreover, they presented an analysis for XACML profile for RBAC model. Ardagna et al (2010) proposed an extension to the XACML rules with two child elements <CredentialRequirements> and <ProvisionalActions>. The former describes the credentials that the requester needs to own and the conditions that must be satisfied. The latter describes the actions that the requester has to perform.

Ran & Guo (2011) integrated a traditional XACML and scalable SOAP message-level security strategy to construct a security XACML access control model based on SOAP encapsulate (S-XACML). In their model, the XACML message is packaged into a SOAP message. Patel & Atay (2011) proposed an access control model, namely, XML to Relational Authorization Rule (X2RAC) for relational storage of the XML documents. Their model permits the security administrators to specify all the authorization information in XML, and store them into relations. Mourad et al (2011) proposed an approach to create XACML policies from XACML profiles. Their approach is based on the preparation of an abstract language on top of an XACML profile specification, which is translated into an XACML policy, using their compiler. Xu et al (2011) proposed an XACML-ARBAC profile to specify Administrative Role Based Access Control (ARBAC) polices. Moreover, they extended the Sun's XACML architecture by developing an Administrative Policy Enforcement Point (APEP) and a Lock Manger to provide the security features of a policy management.
Stepien et al (2011) proposed the non-technical XACML presentation notation, to ease the complexity of policy rules. Farooqi & North (2011) used the trust-based access to XML databases. In trust-based access control, threats are detected, user privileges are calculated dynamically depending on the users trust value, and the access decision is depended on matching the node trust value and the user trust value. Ma et al (2011) proposed an architecture for sharing information cross social networks, based on XACML securely and effectively. An & Park (2011) proposed an efficient access control labeling scheme. Their schema is used for processing XML queries under dynamic XML data streams securely. Their schema is based on the dynamic roles generated using prime number and group-based prime number labeling schemas where labels are encoded with ancestor-descendant and sibling relationships between nodes. Luo et al (2011) proposed an efficient technique, named QFilter, based on Non-Deterministic Finite Automata (NFA). Their technique translates the user's insecure queries into secure ones, without violating the access control rules.

Li & Fan (2012) proposed a combination of the RBAC model and a specific credit management system, to instantiate the model. Moreover, they used UML to explain the model, and XACML to explain the access permission between the users and objects. Chae et al (2012) proposed role attributes for access control in XML databases in which attributes are used to specify the characteristics of a role. Their method extends the XACML RBAC profile to support role attributes by proposing new entities, namely, Role Attribute Point (RAP) and Extended-PIP (E-PIP). RAP is used to manage the proposed role attributes. Extended-PIP (E-PIP) is an extension of the Policy Information Point (PIP) of XACML. It is connected to RAP to deal with role attributes. Farooqi & North (2012) used the Xlog file as a dynamic and temporary log file for XML databases. They used the Xlog files to evaluate user' behavior by recording user' transactions and errors.
Yang & Liu (2012) proposed an action type of access control model. Their model defines the type of behavior to solve the problem of the access model. Xin-fang & Xiao-hua (2012) proposed an extension to the attribute-based access control model using hidden credentials technology. Their extension provides the cross protection of sensitive attributes and strategies to perform attribute-based access control. Chebotko et al (2012) classified the access control models to the XML documents into XPath-based and DTD-based model. They defined each class and listed the advantages and disadvantages for each class. Moreover, they proposed the first DTD-based access control model that exploited the graph matching to analyze if an input query is fully acceptable, fully rejectable, or partially acceptable. Therefore, the fully acceptable and rejectable queries are not needed for checking. However, the partially acceptable queries will be rewritten into an equivalent recursive query or into a non-recursive query.

Stepien et al (2012) proposed an algorithm that used a recursive process of subsumption carried out on the original set of policies for reducing the size of access control policies in XACML. The reduced policy sets decrease the risk of conflicts and improve PDP performance. Thi & Dang (2012) proposed an access control model, namely, eXtended XACML for Spatial Temporal Role based access control model with OWL (X-STROWL). They combined XACML and OWL ontology for providing the NIST standard RBAC model with new data types and functions. Bravo et al (2012) presented techniques to solve inconsistent full and partial policies. They proposed approximate algorithms and showed that, they got reasonable results in practice. Moreover, they evaluated the algorithms and showed that, the consistency and insert–update-delete repair algorithms are running fast and effectively. Ulltveit-moe & Oleshchuk (2012) proposed a decision cache for fine-grained XACML authorization and anonymization of elements and
attributes in the XML documents. Their model permits for management of authorization and anonymization policies for the XML documents.

Thimma et al (2013) proposed a hybrid XML access control mechanism, namely, HyXAC. The proposed technique uses QFilter approach to process queries. It defines a sub-view for each access control rule. Moreover, it allocates dynamically the available resources to materialize and cache sub-views to improve query performance. Laborde et al (2013) studied the using of XACML for Authorization as a Service in the cloud security community. Bertolino et al (2013) proposed a set of mutation operators to check the faults of the XACML 2.0 policies. Moreover, they proposed a tool, called XACMUT (XACmlMUTation), for creating mutants. Lin et al (2013) proposed a policy similarity measure approach, to determine similar policies.

2.3 PROPOSED WORK

In spite of all these works, the temporal attributes were considered as any other attributes. However, it is necessary to consider the temporal attributes as special attributes, due to their importance in many applications. In addition to the temporal attributes, the security features of XML databases are violated or tampered with by malicious users. Therefore, secure and temporal oriented algorithms are proposed in this research work, to enhance the security and applications' requirements.

Moreover, none of these works focused on how to overcome the complex structure of XACML, which is useful to express and interchange access control policies and requests/responses effectively. Hence, this research proposes new algorithms for mapping XACML policies and rules into relational rules, and storing them in the form of rules in temporal relations, to ease the access control to the XML documents. This proposed work relieves the users from the effort of learning and understanding the
XACML policies and rules; hence, it reduces the users' time and effort. It controls the access to the XML documents stored in either native or relational databases, using the XACML policies. Finally, it applies the constraints of rules, and obligations and provides the response to an access request effectively.

The second contribution of this research work is proposing a new time-stamp based algorithm, for decrypting the encrypted XML documents partially. This proposed algorithm utilizes a new temporal model for XML representation, based on a combination of valid time and transaction time, through the tuple time-stamping. Moreover, one attribute of the key components of the encrypted elements is selected to distinguish among them. The time-stamp and the selected attribute guide the receiver to decrypt the required parts of the encrypted XML documents, instead of decrypting all the parts of them. Moreover, they can be used to retrieve the parts that must be decrypted, to contribute to the query results on the encrypted XML documents. The proposed algorithm not only reduces the decryption time, but also protects the security of the data.

2.4 SUMMARY

This chapter presents a literature review of XML security (signature and encryption) and access control to the XML documents. This survey explains that, the temporal attributes were not considered as special attributes, the security features of XML databases are violated or tampered with by malicious users, and there is no proposal about how to overcome the complex structure of XACML, which is useful to express and interchange access control policies and requests/responses effectively.