An Efficient Technique for Detection and Prevention of SQL Injection Attack in Cloud Computing

Miss. S. P. Dhanorkar, Dr. V. M. Thakare, Dr. S. S. Sherekar

SGBAU, Amravati, Maharashtra, India

ABSTRACT- Structured Query Language (SQL) injection and Cross Site Scripting Attack (XSS) is one of the most common application layer attack used by attacker to deface the website, manipulate or delete the content through inputting unwanted command strings. SQL injection attack is one of the most serious security vulnerabilities in Web application system. Most of these vulnerabilities are caused by lack of input validation and SQL parameters use. This paper proposes typical SQL injection attack analysis and prevention technologies. This paper focused analysis of five different techniques such as novel identity-based and proxy re-encryption, Service Level Agreement security detection, Cloud-Trust, Partial Lagrange multiplier technique, A Contract Design technique. To improve these techniques the new method is proposed here that is "Enhanced security using sql injection attack".

Keywords—*SQL Injection Attack, Apriori strategy, Prevention and Detection, Security as a Service AES Algorithm*

I) INTRODUCTION

Cloud computing is a new service model which has a great development with the advantages of flexible configuration, on-demand purchase and easy-maintenance. It also brings a huge challenge to the security services. A data-centric approach is used for data self-protection, where novel cryptographic techniques such as Proxy Re-Encryption Encryption (PRE) are used. This approach can help to control and manage security and to deal with the complexity of managing access control in Cloud computing [1]. Cloud computing is a computing model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and other services) that can be rapidly provisioned and released with minimal management effort or cloud service provider (CSP) interaction. One way to implement this would be for the cloud service provider to sign a service level agreement (SLA) to identify the privacy requirement from SC [2]. Virtualization, the basis for most CCSs, enables CSPs to start, stop, move, and restart computing workloads on demand. VMs run on computing hardware that may be shared by cloud tenants. This enables flexibility and elasticity, but introduces security concerns [3]. Despite the variety of security options available, it is inevitable that they will eventually be circumvented. Cyber insurance is used to provide explicit cover in the event that malicious activity leads to financial loss [4]. A cloud-enabled IoCT allows heterogeneous components to provide services in an integrated system. For example, cloud resources can provide data aggregation, storage and processing for the physical systems. The sensors associated with devices1 can send data to the remote controllers through up-links, and the control commands can be sent back to the actuator via downlinks [5]. This paper, discusses different Security Technique such as Novel identity-based and proxy re-encryption, Service Level Agreement security detection, Cloud-Trust, Partial Lagrange multiplier technique, A Contract Design technique. But these techniques also have some problem so to overcome such problems improve security of cloud is proposed here that is **"Friendly enhanced security using sql injection attack"** with apriori algorithm and AES algorithm.

II) BACKGROUND

Many studies on Security of Cloud Computing have been done in recent past years such Techniques are: Novel identity-based and proxy re-encryption techniques are used to protect the authorization model. Each piece of data is ciphered with its own encryption key linked to the authorization model and rules are cryptographically protected to preserve data against the service provider access or misbehaviour when evaluating the rules [1]. Service Level Agreement security detection technique is devised for the maintenance of the user's security in a cloud computing environment. SLA based Privacy Protection Model (SLA-BPPM) is devised for the maintenance of the user's privacy in a cloud-computing environment. This is based on a Markov decision-making process, which is introduced for modeling according to the users' privacy requirements in the SLA, which can result in the permission of CSP operation [2]. A cloud security assessment model—Cloud-Trust—that provides quantitative high level security assessments of IaaS CCSs and CSPs. Cloud-Trust can assess the relative level of security offered by alternative CSPs or cloud architectures [3]. Partial Lagrange multiplier technique that improve the security of cloud. Customer runs applications that assume to be Internet-accessible that provide security [4]. A Contract Design Approach. Develop contract design technique to propose an integrative cyber-physical framework to develop a security as a service mechanism for real time operation of cloud enabled IoCT under APTs [5].

This paper introduces five Security improvement techniques ie Novel identity-based and proxy re-encryption techniques are used to protect the authorization model, Service

Level Agreement security detection technique, Cloud-Trust technique CCS reference architecture and a cloud security assessment technique, Partial Lagrange multiplier technique and contract design technique using Bi-Level system are organizes as follows. **Section I** Introduction. **Section II** discusses Background. **Section III** discusses previous work. **Section IV** discusses existing methodologies. **Section V** discusses attributes and parameters and how these are affected on security techniques **Section VI** proposed method and outcome result possible. Finally **section VII** Conclude this review paper.

III) PREVIOUS WORK DONE

Juan M. et al (2017) [1] has proposed Novel identity-based and proxy re-encryption techniques are used to protect the authorization model. Data-centric solutions based on novel cryptographic mechanisms applying Attribute based Encryption (ABE) these solutions are based on Attribute-based Access Control (ABAC), in which privileges are granted to users according to a set of attributes. control policy is defined by the data owner for its data.

Shengli Zhou et al (2017) [2] has proposes an Service Level Agreement security detection technique is devised for the maintenance of the user's security in a cloud computing environment Service level agreement (SLA) security detection Privacy Protection technique (SLA-BPPM) is devised for the maintenance of the user's privacy in a cloud-computing environment. This is based on a Markov decision-making process, which is introduced for modeling according to the users' privacy requirements in the SLA, which can result in the permission of CSP operation.

Dan Gonzales et al (2017) [3] has proposed the Cloud security assessment model—Cloud-Trust technique—that provides quantitative high level security assessments of IaaS CCSs and CSPs. Cloud-Trust can assess the relative level of security offered by alternative CSPs or cloud architectures.

Jonathan Chase et al. (2017) [4] proposed Partial Lagrange multiplier techniques that improve the security of cloud. Customer runs applications that assume to be Internet-accessible that provide security Security-as-a-Service approach as a way of securing cloud-based data through encryption and distribution of data addresses.

Juntao Chen et al. (2017) [5] proposed A Contract Design approach. Develop contract design technique to propose an integrative cyber-physical framework to develop a security as a service mechanism for real time operation of cloud enabled IoCT under APTs.

IV) EXISTING METHODOLOGIES

A Novel identity-based and proxy re-encryption techniques

Novel identity-based and proxy re-encryption techniques are used to protect the authorization model. Data is encrypted and authorization rules are cryptographically protected to preserve user data against the service provider access or misbehavior.

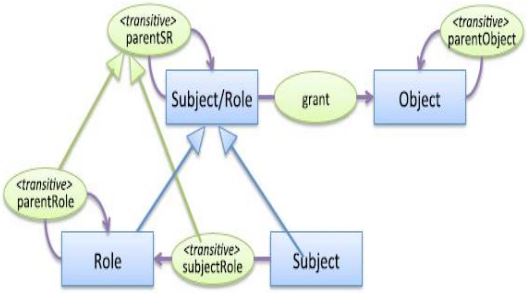

Fig.1. Ontology representing authorization model.

Each piece of data is ciphered with its own encryption key linked to the authorization model and rules are cryptographically protected to preserve data against the service provider access or misbehaviour when evaluating the rules.

B Service Level Agreement security detection

privacy based SLA Security detection technique a way to measure concerns about the security of QoS in cloud computing, in which users can judge the reliability of a CSP and choose a Suitable one if their requirements are not met. A SLA forms a bridge between the CSP and users and focuses on QoS.

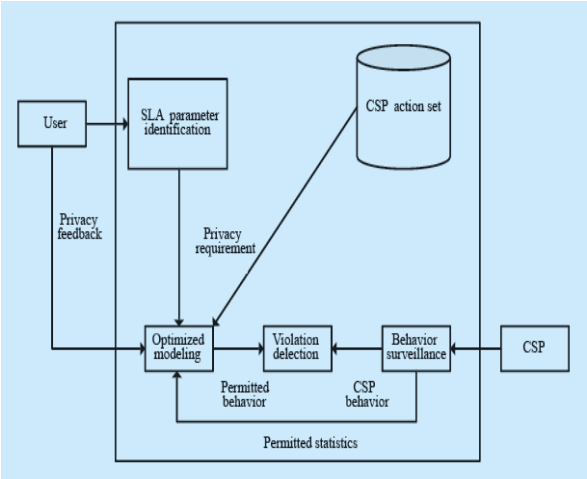

Fig.2. SLA-BPPM functional framework

SLA-BPPM can better recognize the violation behaviour and possess good practically.

C Cloud-Trust technique

The Cloud-Trust technique is devised for the maintenance of the user's security in a cloud computing environment Service level agreement (SLA) security detection Privacy Protection technique (SLA-BPPM) is devised for the maintenance of the user's privacy in a cloud-computing environment The Service level agreement (SLA) technique. The human-machine interaction is implemented using an XML file as commonly applied in web services.

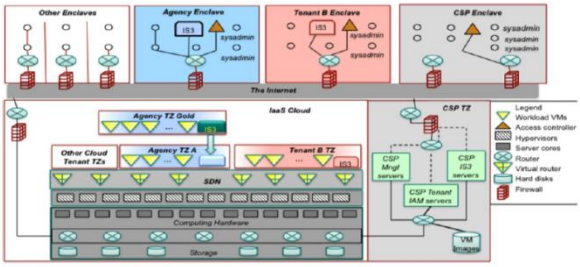

Fig.3. CCS reference model

It provides two key high-level security metrics to summarize CCS security status quantitatively a cloud security assessment model—Cloud-Trust—that provides quantitative high level security assessments of IaaS CCSs and CSPs. Cloud-Trust can assess the relative level of security offered by alternative CSPs or cloud architectures.

D Partial Lagrange multiplier technique

partial Lagrange multiplier technique that takes advantage of the total unimodularity property to find the solution in polynomial time.Security-as-a-Service (SECaaS) technique was introduced in, where it was proposed as a way of securing cloud-based data through encryption and distribution of data. addresses the problem of selecting cloud service providers (CSP) with security considerations as a priority. The full Lagrange multiplier method is an established technique for solving convex optimization problem using linear constraints as in the following equation.

$$\min_{\vec{\mathbf{x}}} f_0(\vec{\mathbf{x}}) \left| \begin{array}{l} f_i(\vec{\mathbf{x}}) \leq 0,\ i = 1, \ldots, m; \\ h_i(\vec{\mathbf{x}}) = 0,\ i = 1, \ldots, p, \end{array} \right.$$

$$L(\vec{\mathbf{x}}, \vec{\boldsymbol{\lambda}}, \vec{\mathbf{v}}) = f_0(\vec{\mathbf{x}}) + \sum_{i=1}^{m} \lambda_i f_i(\vec{\mathbf{x}}) + \sum_{i=1}^{p} v_i h_i(\vec{\mathbf{x}}),$$

E Contract design technique

A Contract Design technique to propose an integrative cyber-physical framework to develop a holistic incentive-compatible and cost-efficient security as a service mechanism for real-time operation of cloud-enabled IoCT under APTs. Author compose the Flip Cloud game with the contract design through a bi-level game model to capture the strategic interactions between the service provider, the device and the adversary.

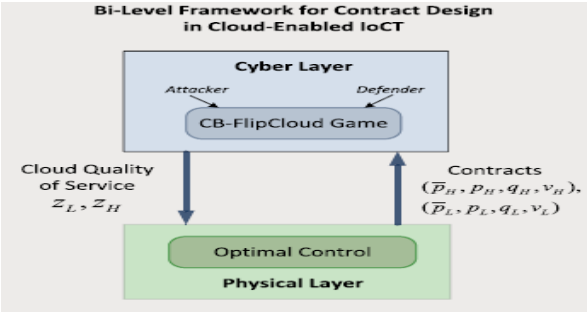

Fig.4. Bi-Level Framework for contract design in Cloud-Enabled loCT

V) ANALYSIS AND DISCUSSION

Novel identity-based and proxy re-encryption techniques are used to protect the authorization model. Data is encrypted and authorization rules are cryptographically protected to preserve user data against the service provider access or misbehaviour. Data centric access techniques are used to protect both the data and the authorization model [1]. privacy based SLA Security detection technique a way to measure concerns about the security of QoS in cloud computing, in which users can judge the .Improve the posterior test for SLA's management [2]. The Cloud-Trust technique is devised for the maintenance of the user's security in a cloud computing environment Service level agreement (SLA) security detection Privacy Protection technique (SLA-BPPM) is devised for the maintenance of the user's privacy in a cloud-computing environment. Cloud Security assessment techniques Provide high level security assessments of Iaa [3]. Partial lagrange multiplier algorithm proposed Optimization involves solving an integer programming problem. Securing cloud based data through encryption and distribution of data [4]. Contract design technique enables an on-demand service provision of security and a pricing mechanism to service real-time cloud-enabled IoCT. This SaaS paradigm provides reliable ways to deliver critical IT services to future IoTs [5].

Security techniques	Advantages	Disadvantages
Novel identity-based and proxy re-encryption	Control and manage security and to deal with the complexity of managing access control in cloud computing.	1. Big challenge for a data-centric approach since data has no computation capabilities by itself. 2. Modify and delete actions are not used.
Service Level Agreement security detection	Improve security using service level agreement violation detection model.	It requires the cooperation of the CSP for its operation and the users' role setting also needs to be determined afore hand..
Cloud-Trust	Advantage of VM co-residency, which arises when VMs of two or more users share the same hardware. If the attacker's VM is co-resident with the target VM it may be able to glean information.	It also does not include all possible insider attack vectors and methods.
Partial Lagrange multiplier technique	1. Optimization involves solving an integer programming problem. 2. Securing cloud based data through encryption and distribution of data.	More expensive
A Contract Design technique	Asymmetrical information is an important feature of contract design problem	Problem of devices, need to establish a holistic framework that integrates cyber physical layers in IoCT together

TABLE 1: Comparisons between different security techniques

PROPOSED METHODOLOGY

Friendly enhanced security using sql injection attack

SQL injection attacks pertain to a class of attacks in which user input is molded in such a way so that a part of the query provided by user is SQLIA code. Thus SQLIA tricks the database by passing malicious code to database by embedding it with user input. The attacker injects pieces of malicious software into the databases, which when processed cause data to be executed as a part of command at the backend server, therefore giving undesired results, which are not anticipated by developers leading to compromised security. Objective of this paper is to To re-design the existing available cloud system for running the sqlia detection and prevention. To detect sql injection attacks performing its prevention by implementing Apriori algorithm.

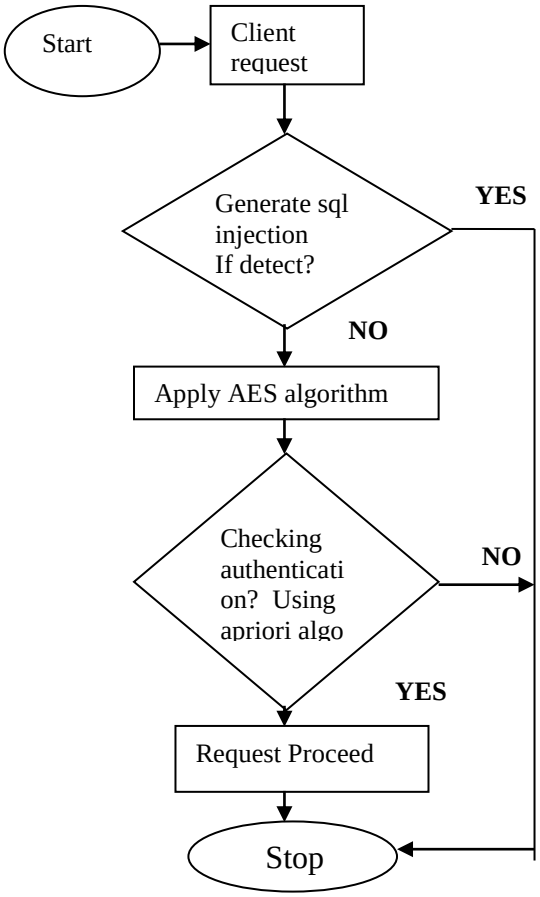

Fig.5. Friendly enhanced security using SQL injection attack

For security purpose used AES algorithm to modify and update the user Authentication window to detect sql injection attacks and identify the intruder.

Apriori is an algorithm for frequent item set mining and association rule learning over transactional databases. It proceeds by identifying the frequent individual items in the database and extending them to larger and larger item sets as long as those item sets appear sufficiently often in the database. The frequent item sets determined by Apriori can be used to determine association rules which highlight general trends in the database.

Algorithm:

Steps:

Step 1: Start

Step 2: Request from client

Step3: Generate sql injection

If detect go to Step 7

Else go to next Step

Step4: Apply AES algorithm

Step5: Checking Authentication

If authenticate go to next Step

Else go to Step 7

Step6: Request proceed

Step7: Stop

OUTCOME AND POSSIBLE RESULT

The proposed method "Friendly enhanced security using sql injection" will be successfully improves the security of the cloud. It also includes all possible insider attack vectors and methods.

VII) CONCLUSION

The SQL Injection Attack is the largest accessible security risk in the network based computer database in today because all attacker or application programmer attempt to crack the information safety measure accepting similar form of violation. In such a manner this proposed scheme regarding security against SQLIA, is too sensitive. In this paper propose the method to detect and prevent the SQL injection by using Apriori algorithm technique and for security purpose use AES algorithm.

FUTURE SCOPE:

SQL injection attack with AES and apriori algorithm successfully implemented. In future work include the extension of the current framework by considering the continuous type of cloud service provider and quantifying the value of asymmetric information and further improve the efficiency while keeping all nice features of the system.

REFERENCES

[1] Juan M. Marın Perez, Gregorio Martınez Perez, and Antonio F. Skarmeta Gomez, "SecRBAC: Secure data in the Clouds," IEEE

TRANSACTIONS ONSERVICES COMPUTING, VOL. 10, NO. 5, SEPTEMBER/OCTOBER 2017.

[2] Shengli Zhou, Lifa Wu, Canghong Jin, "A Privacy-Based SLA Violation Detection Model for the Security of Cloud Computing," IEEE September 2017.

[3] Shengli Zhou Dan Gonzales, Member, IEEE, Jeremy M. Kaplan, Evan Saltzman, Zev Winkelman, and Dulani Woods, "Cloud-Trust—a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds," IEEE TRANSACTIONS ON CLOUD COMPUTING, VOL. 5, NO. 3, JULY-SEPTEMBER 2017.

[4] Jonathan Chase, DusitNiyato, Ping Wang, SivadonChaisiri, Ryan K L Ko, " A Scalable Approach to Joint Cyber Insurance and Security-as-a-Service Provisioning in Cloud Computing," IEEE Transactions on Dependable and Secure Computing, 2017.

[5] Juntao Chen, Student Member, IEEE, and Quanyan Zhu, Member, IEEE," Security as a Service for Cloud-Enabled Internet of Controlled Things Under Advanced Persistent Threats: A Contract Design Approach," IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 12, NO. 11, NOVEMBER 2017.