Section A-Research paper

Web Application Security Threats: SQL Injection Attack

Dr. Smita Chavan[1] Dr, Pratibha Jadhav [2] Dr. Rupali Mahajan[3] Dr. Kaushalya Thopate [4]

[1] Information Technology Department ,Government College of Engineering, Aurangabad, India, rathod.sb@gmail.com

[2] Applied Science and Humanities Department, School of Engineering and Science MIT-Art Design and Technology, Pune, India pratibhajadhav1@gmail.com

[3] Computer Engineering Department, Vishwakarma Institute of Information Technology, Pune, India rupali.mahajan@viit.ac.in

[4] Department of Computer Engineering , Vishwakarma Institute of Technology,Pune India Kaushalya.thopate@vit.edu

***Abstract*—HTTP Vulnerability is an important security threat in this era. Currently attacks like SQL and DOS attacks are utmost common threats originate in the web applications. Mostly web application security vulnerabilities are SQL injection in which statements from SQL are reformed by attackers which is accomplished by applications over the web and presented to the server containing database. This type of attack is happening direct to lack of parameters used in SQL used and validation of input. Different type of latest web application attacks are SQLi, cross site scripting, session management and broker authentication , security misconfiguration ,insecure direct object references, , CCRF are identified in this paper. System developed attack identification and detection of SQL injection attack by using cloud service provider. This paper shows infrastructure on the cloud with virtual machine. Security groups are created to monitor the network traffic as inbound and outbound. Some test cases are performed to identify and detect such a type of attacks. Different pattern of attacks are considered. Risk and challenges of SQL injection attacks are mentioned.SQL injection attack model performance is shown in the system.**

***Index Terms*— HTTP Vulnerability, Web Application Attacks, Cloud Service Provider, Virtual Machine, SQLi performance.**

I. INTRODUCTION

Nowadays every third person is connected to internet. This exposure to internet brings a threat to his/her data security. Attackers are active more than earlier as people are not too much IT literate or even in some cases systems are not full proof. So, there is a need to consider web application security. Obviously if there is concept of web application security, it is related to cloud security. In this paper challenges of cloud security are studied according to threats, needs and current survey of cloud security. Cloud security research areas are considered like virtualization, cloud security dimensions, data security, data separation, encryption, denial of service, DDoS Attacks etc. Characteristics of cloud security are achieved in terms of data security, data integrity, data confidentiality, scalability, better performance, and resource pooling. Many users upload their data on cloud or on different websites, so data security is important and is to be achieved. By using security rules there is no scope for malicious modification and integrity is maintained. Data confidentiality is information centric for secure transfer of files. If cloud service provider is used, resources can be scale up or scale down as per application need. Obviously by using cloud and any CSP system can achieve better performance. Resource pooling is like reserving resources for the application and after usage resources are released. In this paper detection of malicious traffic is done with the help of protocols and

vulnerability ontology. Hence identification of HTTP vulnerability attacks like DDoS attacks are detected. Finally with the help of local host and cloud time and space complexity is achieved.

II. RELATED WORK

Most of the papers have presented identification and detection of web application attacks by using SQL injection attack. Ref. [1] shown prevention, detection and demerits of SQL injection attacks by using cloud computing service provider's firewall. Cloud database contents are authorized through several checkpoints. The security of the database is maintained by these checkpoints. These checkpoints can be harmed by the SQLIA at any of the service (EaaS, DaaS, SaaS, IaaS, PaaS,). Methods used provides resource sharing over wide access of network between different users, this will result availability of resources as per need to provide data security. Ref. [2] showed the performance of the system by tokenizing the user input query ex. double dashes, white space, sharp sign and so on. Every single string token was identified through the content of lexicon predefined () most of reserved words commands and some logical operators. Injected commands like after concept drop, delete execute, sleep, shut down, union, or if. System performed few queries of sql injection on query statements vulnerable like 10 tested queries among them 3 are normal and 7 are injected. This system is applied for effective avoidance from various queries(malicious) for insertions. Ref. [3], performed attack detection method of the SQL injection by deleting the SQL query parameter values is examined and findings are shown. Extra research is essential for accurate SQL injection attacks detection . These methods are used from detecting and checking originality. System combines dynamic as well static analysis. At dynamic Parameter values are removed and associated by analyzing with SQL query. After removal of the parameter values comparison is done for both.query is normal when both values are same, if not same then the query is not normal. Ref. [4] detected attacks of vulnerability triggered because of performed input by different users those are not validated properly crosswise the application of web , proposed application done identification of attacks but not focused-on protection of data from threats and attacks in web applications. Different types of attacks are studied like XSS mechanism of analyzer detection, validation of protocol for attacks, SQL injection, buffer overflow. Authors also analyzed malicious attacks by suggesting mitigation and prevention of attacks. Ref. [5] gives standard injection attack of SQL and technologies related to prevention,, which are introduced input validation are not done on all parameters by providing methods. It shows characteristics of prevention methods and SQL injection attack. This type of attack can be presented by validation of input parameter methods like type safe SQL. Defense model is proved to inhibit injection attacks of SQL by assessing the size of input ,queries intended with the actual queries. The method can be used for defending application of web.

III. METHODS

System developed by using both ways local host and cloud. Software's used are putty, winSCP, fiddler tool and protégé tool. Putty is used to connect remote machine with local machine by using some commands. These commands used to check status of remote machine, to get IP address of remote machine. WinSCP i.e., windows secure copy protocol is Microsoft clients to transfer files securely between local machine and remote machine. Fiddler tool is open source used to capture network traffic of local machine and remote machine .It is associated with web application firewall WAF. AWS services used from elastic computing cloud EC2 like IAM, MFA, Modsecurity. With a bunch of service of EC2 it is easy to create infrastructure needed to write rules for security. Ref. [6] used virtual machine network traffic can be analyzed. Identity access management is used for roles of users. Multifactor authentication code is attached to particular security group. Modsecurity is nothing but web application firewall. It is used with by default rules or users can create their own rules. As per ref. [7], once environment setup is ready on virtual machine, firstly testing is done on local machine. It uses MVC architecture of java i.e., model view and control. To give protection to the system functions are used to identify and detect attacks. Ref. [8] shown attacks like ICMP, HTTP, TCP, UDP and

private port attacks. Ontology rules are written for inbound, outbound, JSON and policy rules. Inbound is for incoming traffic from anywhere i.e. source. Outgoing traffic is for outgoing to anywhere i.e., destination. Java script object notation is used to store key value pairs in the form of pointer values. Ref. [9], [10] Policy rules are based on automated rules like tailor rule. Overall rules are written by creating security groups.

A. SQL-Injection Attack (Injection Flaws)

HTTP Vulnerability: SQL injection attacks and DOS attacks are two furthermost significant security threats initiated in applications over the web. one of the web application security vulnerabilities are SQL injection in this statements of SQL are changed by attackers which is accomplished by application over the web and presented to the server containing databases. This type of attack is initiated due for lack of input validation and parameters of SQL . Different type of latest web application attacks is SQLi, , broker authentication and session management, cross site scripting insecure direct object references, security misconfiguration, CSRF [13][14].

B. Attack Patterns Example

These are classified into attack types and attack payload string. Tautology

'OR' '1'='1' Line Comment ') or '1'=1-- Bypassing login screens Admin '—

C. Risk & Challenges of SQL Injection Attack

To prevent insecure deserialization vulnerabilities, developer should,

- Sanitize serialized object data as user input like untrusted via filtering or validation.
- Implement integrity check like digital signatures or any serialized object. This will inhibit tampering.
- Finally by isolating run code that deserializes in a low privileged environment [15][16].

D. SQLi Detection and Prevention Techniques Detection Mechanism:

➢ Detection Mechanism:

- Injection through user input.
- Vulnerability scanning and security testing.
- Web application firewalls.
- Secure development training.

➢ Prevention Mechanism:

- Train and maintain awareness.
- Don't trust any user input.
- Adapt to the latest technologies.
- Scan regularly.
- Implement WAF in front of the application.
- Integrate WAF in web server as well use cloud based WAF.

E. HTTP Response Splitting Attack

Attack happens when:

- Entry of data to a web application through source which is untrusted, highly often an HTTP request.
- The data is entered in an HTTP response header transmitted to a user of web without being validated for malicious characters.
- In the proposed system implementation is not done for detection of HTTP response splitting attack.
- Design patterns to create domain ontology are semantic rules.

- Described ontology pattern for SQLi attack is reusable so it can also be applied for HTTP response splitting attack.

IV. RESULTS

a. Environment setup

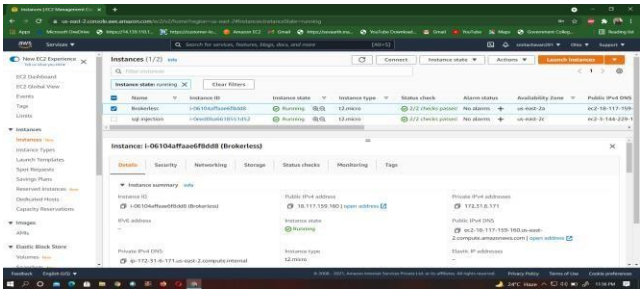

Figure.1. AWS (EC2) Instance Creation Steps and Configuration

As per above fig.1 virtual machine is created i.e. instance on AWS.It will give instance id, type.in the diagram instance state is shown as running. Instance type is t2 micro. Status check is 2/2 that all services related to this virtual machine working properly. If user wants to set alarm for notification it can be possible. Availability zones are shown with its public IPv4 DNS address [17][18][19].

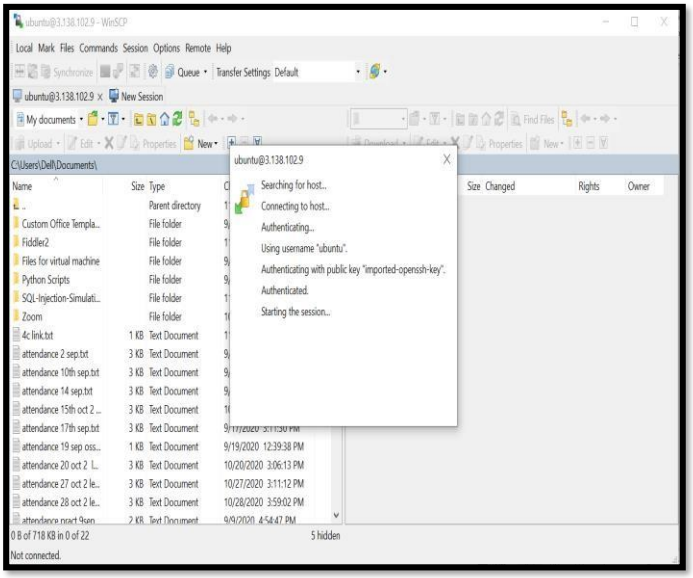

Figure.2-a. Local host Connectivity

Fig.2 (a) shows local host connectivity by using windows secure copy protocol. With WinSCP Putty option local machine is connected to virtual machine. Session will start by entering few of the commands and it will give IP address of connected remote machine [20][21].

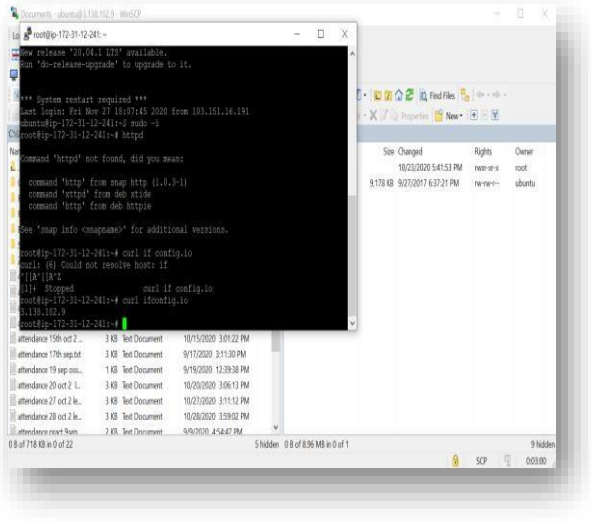

Figure.2-b. Local host connectivity

As per Fig.2 (b) system can analyze configurations of virtual machine. It uses fiddler tool as debugger to capture network traffic. Hence it will show header status either empty or ok. It is possible with IP addresses [22][23].

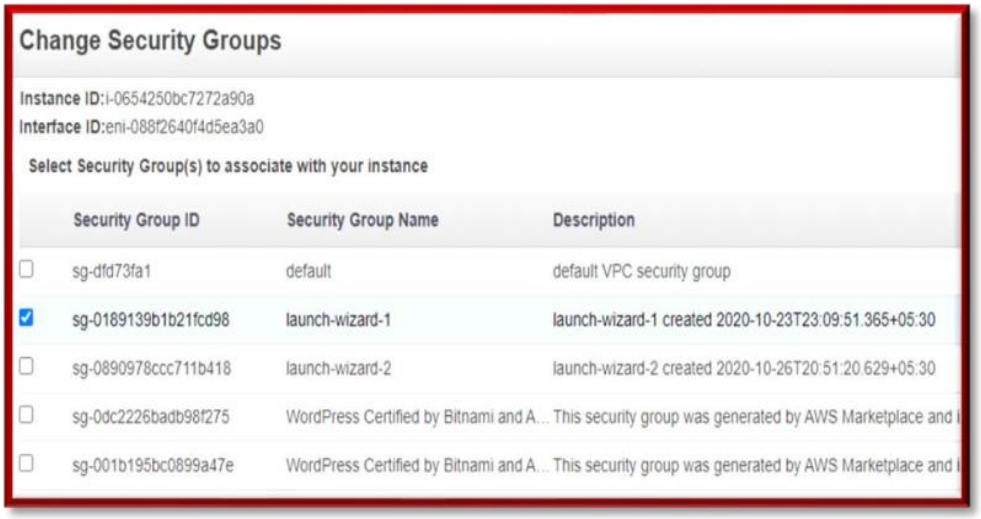

Figure.3. Security group creation

Ref. [11], above diagram fig.3 shows created security groups for virtual machine users. There are two ways to create security group. One is by default from EC2 service. Second by creating own security group. As per

diagram shown instance id security group is attached with security group ID, secutiy group name and its overall description[24][25].

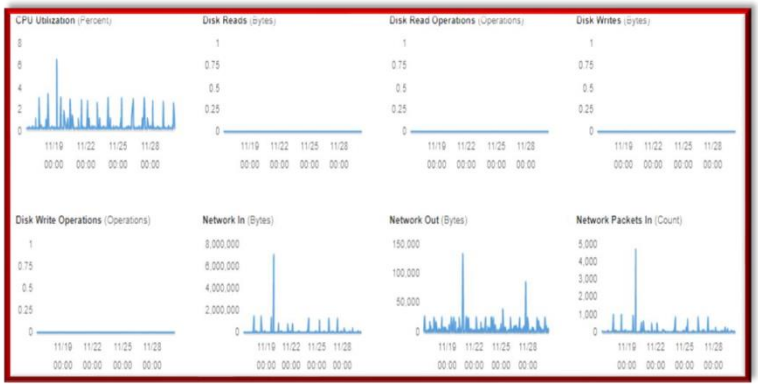

Figure.4. Performance of Virtual Machine

Virtual machine performance can be captured from instance information and its ID as shown in Fig.4.as per the resources used performance is calculated. Figure shows Total CPU utilization, network in bytes, network out bytes as well as total of network packets count [24][25][26].

Table 1: Test cases

Test No.	Test Data	Result	Test Status	Remark
1	Username and Blank Password xie' or '1'--'	Account Balance: 50000	Pass	Without Protection
2	Username and Password is same 1' or '1'='1 1' or '1'='1	User ID or Password is invalid	Fail	With Protection
3	Common user login Username xie Password darren1	Account Balance: 50000	Pass	Without Protection

Ref. [12] as per table 1, above test cases is performed to validate attacks. These cases show identification and detection of SQL injection attacks. Different Methods are used to provide protection. Test performed on intentionally vulnerable web applications example sites; we got SQL injection scanner report as start time, finish time, scan duration and test count. We will also get vulnerable parameter, risk description. Hence performing one test will take 41 seconds [27][28].

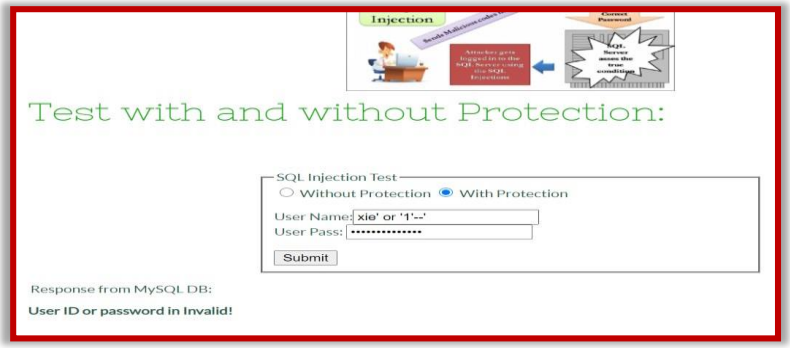

Figure.5. Test Case Execution of SQL Injection Attack

Ref [13] Figure 5 shows result of SQL injection attack. If user will select with protection that means rules are written and if user will select without protection it means without rules. If protection is provided so there is no possibility of attacks and vice versa [29][30].

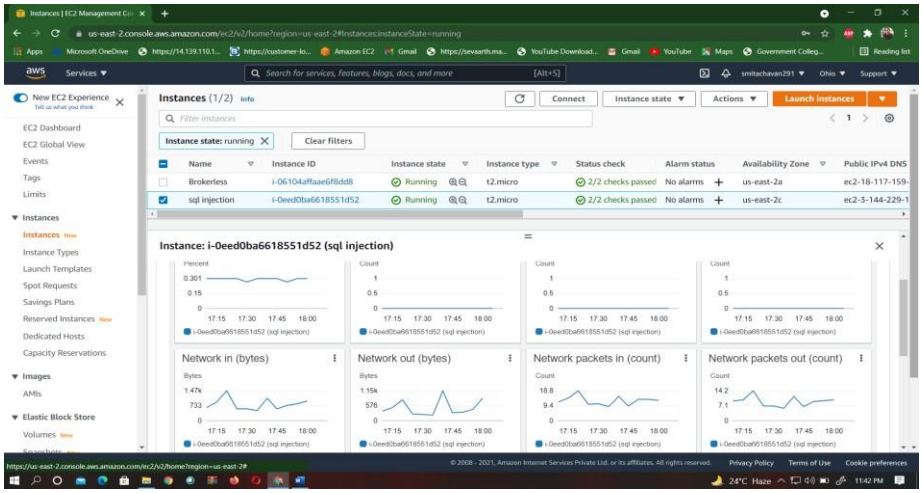

Figure.6.Instance performance by using AWS

Instance performance is observed as per incoming and outgoing traffic to that instance. It is shown in figure 6.

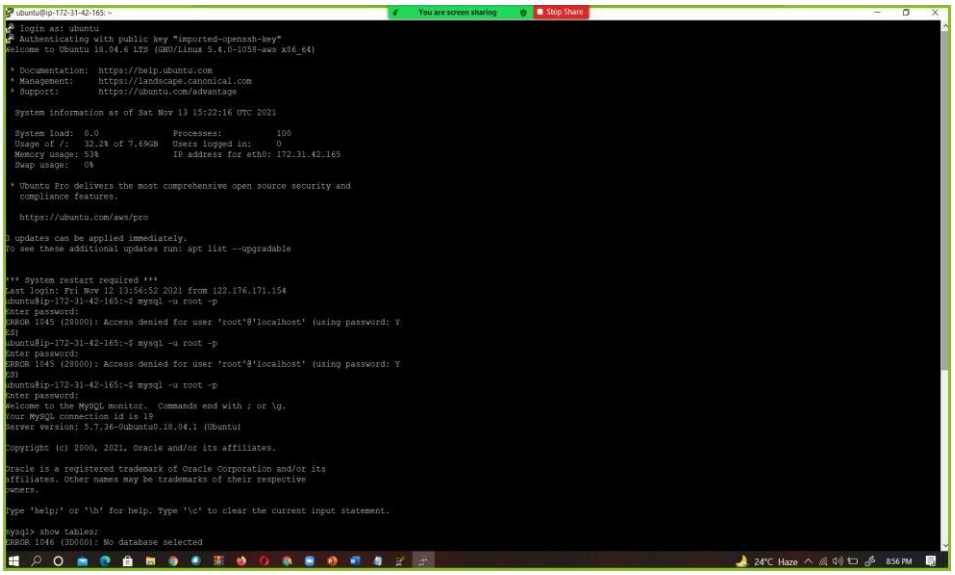

Figure 7-a.Utilization of memory and space with database

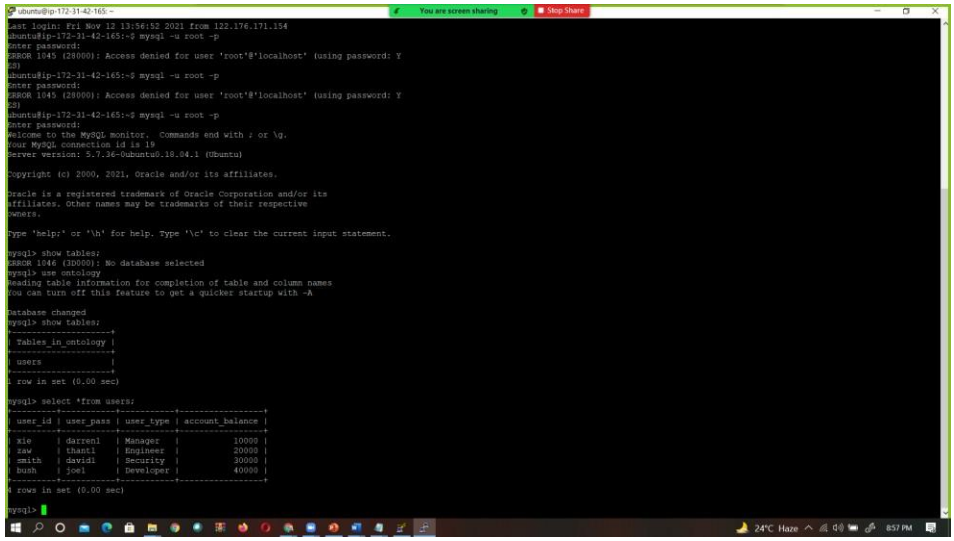

Figure.7-b. Utilization of memory and space with database

Simulation of SQL injection attack module is shown as per fig.7 and b. Execution of workspace analyzed on local host. Calculated Usage 33.2% execution time from 7.69 GB. Observed result is
, Processes=100, Memory Usage=53%, on IP address: 172.31.42.165.

Table 2: Result Analysis

Sr. No.	Previous Work	Proposed Work
Ref(2)	Query fired on username and password.	Query fired on database to extract the data, but some conditions are provided
Ref(3)	SQLIA attack occurred due to SQL parameters used and input validation.	Protection is given to avoid the problem by using validation techniques
Ref(5)	Auto saved username & password	Proposed system provides protection to username and password

SQL Injection Scanner Report Example

http://vulnapp.example.com

Summary

Risk rating

High: 1

Medium: 0

Low: 0

Info: 1

Scan information:

Start time: 2021 11-13 16:47:15

Finish time: 2021 11-13 16:47:56

Scan duration: 41

sec Tests

performed: 2/2

Scan status: Finished

Findings

- SQL Injection

Vulnerable Page	Vulnerable Parameter	Method	Attack Vector
/travel.php	id	GET	http://vulnapp.example.com/travel.php?id=5-2
/bookings.php	cat	GET	http://vulnapp.example.com/bookings.php?cat=4+AND+1%3D1+--+
/user_profile.php	uname	POST	http://vulnapp.example.com/user_profile.php **POST Data:** uname=ZAP' OR '1'='1' --
/user_profile.php	pass	POST	http://vulnapp.example.com/user_profile.php **POST Data:** pass=ZAP' OR '1'='1' --

Risk description:

SQL injection may be possible.

Recommendation:

Do not trust client-side input, still there is client-side validation in place. typically, type checks all data on the server side. If the application uses JDBC, use prepared statement or callable statement, with parameters passed by '?'This does not eliminate SQL injection, but minimizes its impact. Grant the minimum database access that is necessary for the application.

Scan coverage information

List of tests performed (2/2) Spidering target

Scanning for SQL Injection...

Scan parameters Website http://vuInapp.example.com

Scantype: Light Authentication: False

CONCLUSION

The system uses a new approach to ensure authentication and confidentiality. Types of HTTP vulnerability attacks are identified. Simulation of SQL injection attack and identity- based encryption successfully deployed on virtual machine using AWS EC2 services. Hence observed that by using cloud services, deployment of application takes less time with good storage capacity. System gives optimized results on cloud as compared to local machines. System proposed a new attack detection method for web application attacks with HTTP structure. This proposed system is used for sensitive website like banking. In future, this type of application can be used in organization or any industry to detect and prevent web-based attacks. Instead of SQL injection attack other vulnerabilities can be considered to identify and detect attacks.

REFERENCES

[1] S.M.Chavan, Dr.S.C.Tamane,"Demerits, Detection & Prevention of SQL Injection Attacks over the Cloud Computing", International Journal of Psychosocial Rehabilitation, Vol. 24, Issue 06, ISSN: 1475-7192, pp 12499-12507, 2020.

[2] Shravan Singh, Ankit Kumar, "Detection and Prevention of SQL Injection", IJSRE 2020.

[3] R. A. Katole, S. S. Sherekar and V. M. Thakare, Detection of SQL injection attacks by removing the parameter values of SQL query ICISC, pp 736-741, 2018.

[4] Mr. Harshal A. Karande, Miss. Pooja A. Kulkarni, Prof. Shyam," Security against Web Application Attacks Using Ontology Based Intrusion Detection System", IRJET, pp 89-92, 2016.

[5] Li Qian, Zhenyuan Zhu, Jun Hu and Shuying Liu, "Research of SQL injection attack and prevention technology "ICEDIF, pp 303-306, 2015.

[6] S.M.Chavan, Dr.S.CTamane,"Modsecurity: Ontology for Cloud Based Web Service Attacks", International Journal of Advanced Science and Technology Vol. 29, No. 9s, pp. 7766-7773, 2020.

[7] M. Kaur and R. Singh, "Implementing Encryption Algorithms to Enhance Data Security of Cloud in Cloud Computing," Int. J. Comput. Appl., vol. 70, no. 18, DOI: 10.5120/12167-8127, pp. 16–21, 2013.

[8] C. S. Pawar, P. R. Patil, and S. V. Chaudhari, "Providing Security and Integrity for Data Stored in Cloud Storage," 2014 Int. Conf. Inf. Common. Embed. Syst. ICICES 2014, no. February 2014, DOI: 10.1109/ICICES.2014.7033968, pp 1-6, 2015.

[9] M. A. Tariq, B. Koldehofe, and K. Rothermel, "Securing Broker-Less Publish/Subscribe Systems using Identity-Based Encryption," IEEE Trans. Parallel Distributed. Syst., vol. 25, no. 2, DOI: 10.1109/TPDS.2013.256, pp. 518–528, 2014.

[10] A. Diro, H. Reda, N. Chilamkurti, A. Mahmood, N. Zaman, and Y. Nam, "Lightweight Authenticated-Encryption Scheme for Internet of Things Based on Publish-Subscribe Communication," IEEE Access, vol. 8, DOI: 10.1109/ACCESS,2983117, 2020, pp. 60539–60551, 2020.

[11] S S Sankpal, RA Mahajan" A Novel Approach to Improve the Privacy of Information Brokering in Semantic Web " , International Journal of Science and Research (IJSR), volume 3, no.7, 2014

[12] C. Choi, J. Choi, and P. Kim, "Ontology-Based Access Control Model for Security Policy Reasoning in Cloud Computing," J. Supercomputer., vol. 67, no. 3, DOI: 10.1007/s11227-013-0980-1 , pp. 711–722, 2014.

[13] Awasthi, Shashank, Naresh Kumar, and Pramod Kumar Srivastava. "An epidemic model to analyze the dynamics of malware propagation in rechargeable wireless sensor network." Journal of Discrete Mathematical Sciences and Cryptography 24.5 (2021): 1529-1543.

[14] Tyagi, Neha, et al. "Data Science: Concern for Credit Card Scam with Artificial Intelligence." Cyber Security in Intelligent Computing and Communications. Singapore: Springer Singapore, 2022. 115-128.

[15] Sawhney, Rahul, et al. "A comparative assessment of artificial intelligence models used for early prediction and evaluation of chronic kidney disease." Decision Analytics Journal 6 (2023): 100169.

[16] Paricherla, Mutyalaiah, et al. "Towards Development of Machine Learning Framework for Enhancing Security in Internet of Things." Security and Communication Networks 2022 (2022).

[17] Tyagi, Lalit Kumar, et al. "Energy Efficient Routing Protocol Using Next Cluster Head Selection Process In Two-Level Hierarchy For Wireless Sensor Network." Journal of Pharmaceutical Negative Results (2023): 665-676.

[18] Narayan, Vipul, A. K. Daniel, and Pooja Chaturvedi. "E-FEERP: Enhanced Fuzzy based Energy Efficient Routing Protocol for Wireless Sensor Network." Wireless Personal Communications (2023): 1-28.

[19] NARAYAN, VIPUL, A. K. Daniel, and Pooja Chaturvedi. "FGWOA: An Efficient Heuristic for Cluster Head Selection in WSN using Fuzzy based Grey Wolf Optimization Algorithm." (2022).

[20] Faiz, Mohammad, et al. "IMPROVED HOMOMORPHIC ENCRYPTION FOR SECURITY IN CLOUD USING PARTICLE SWARM OPTIMIZATION." Journal of Pharmaceutical Negative Results (2022): 4761-4771.

[21] Babu, S. Z., et al. "Abridgement of Business Data Drilling with the Natural Selection and Recasting Breakthrough: Drill Data With GA." Authors Profile Tarun Danti Dey is doing Bachelor in LAW from Chittagong Independent University, Bangladesh. Her research discipline is business intelligence, LAW, and Computational thinking. She has done 3 (2020).

[22] Narayan, Vipul, et al. "Enhance-Net: An Approach to Boost the Performance of Deep Learning Model Based on Real-Time Medical Images." Journal of Sensors 2023 (2023).

[23] Ojha, Rudra Pratap, et al. "Global stability of dynamic model for worm propagation in wireless sensor network." Proceeding of International Conference on Intelligent Communication, Control and Devices: ICICCD 2016. Springer Singapore, 2017.
[24] Shashank, Awasthi, et al. "Stability analysis of SITR model and non linear dynamics in wireless sensor network." Indian Journal of Science and Technology 9.28 (2016).
[25] Gupta, Sandeep, Arun Pratap Srivastava, and Shashank Awasthi. "Fast and effective searches of personal names in an international environment." Int J Innov Res Eng Manag 1 (2014).
[26] Srivastava, Arun Pratap, et al. "Fingerprint recognition system using MATLAB." 2019 International conference on automation, computational and technology management (ICACTM). IEEE, 2019.
[27] Kumar, Neeraj, et al. "Parameter aware utility proportional fairness scheduling technique in a communication network." International Journal of Innovative Computing and Applications 12.2-3 (2021): 98-107.
[28] Awasthi, Shashank, et al. "A New Alzheimer's Disease Classification Technique from Brain MRI images." 2020 International Conference on Computation, Automation and Knowledge Management (ICCAKM). IEEE, 2020.
[29] Awasthi, Shashank, et al. "Modified indel treatment for accurate Phylogenetic Tree construction." 2020 International Conference on Computation, Automation and Knowledge Management (ICCAKM). IEEE, 2020.
[30] Mohseni, S., Yang, F., Pentyala, S., Du, M., Liu, Y., Lupfer, N., ... & Ragan, E. (2021, May). Machine learning explanations to prevent overtrust in fake news detection. In Proceedings of the International AAAI Conference on Web and Social Media (Vol. 15, pp. 421-431)