International Journal of Research in Advent Technology, Vol.7, No.3, March 2019
E-ISSN: 2321-9637
Available online at www.ijrat.org

Intrusion Detection and Prevention System in IoT Environment

Sweta Dave[1], Prof. Sandip Chauhan[2]
M.E. Final Year Student [1,] Assistant Professor[2], Department of Information Technology [1,2] , Shantilal Shah Engineering College, Bhavnagar,India.[1,2]
Email: sweta.dave15@gmail.com[1] *,sandymba2007@gmail.com*[2]

Abstract-Internet of Things (IoT) may be a new paradigm that integrates the net and physical objects to totally different domains like home automation, process, human health and environmental observance. It deepens the presence of Internet-connected devices in our daily activities, bringing, additionally to several advantages, challenges associated with security problems. For quite 20 years, Intrusion Detection Systems (IDS) are a vital tool for the protection of networks and data systems. However, applying ancient IDS techniques to IoT is troublesome because of its explicit characteristics like constrained-resource devices, specific protocol stacks, and standards. In this paper, we tend to gift an in depth review on various kind of SQL injection attacks, vulnerabilities, and interference techniques. Aboard presenting our findings from the survey, we tend to conjointly compose future expectations and attainable development of countermeasures against SQL injection attacks.

Index Terms-SQL Injection, Sensor, IOT, Attack.

1. INTRODUCTION

The IoT is a smart network which connects all things to the Internet for the purpose of exchanging information and communicating through the information sensing devices in accordance with agreed protocols. Which achieves the goal of smart identifying, locating, tracking, monitoring, and managing things.[10]

Current smart devices such as routers and cameras, have suffered malicious attacks from hackers. Therefore, for the purpose of improving security defensive capability of IoT is an urgent need.[10] The IoT technology has changed people's life style due to information collection, communication, and processing abilities. In the development of the Internet-of-Things, one of the major obstacles is security and privacy issues. IoT attacks may cause privacy violation and threaten people's life and privacy safety. Protecting the privacy of users has become another important challenge in the development of IoT [5]. Among the various types of attacks affecting IoT devices, the major threat is to protect the data captured by the IoT devices and stored in to the server. This type of attack is known as SQL Injection attack[12].

By embedding SQL statements into the input data, a poorly designed program may be vulnerable to such attacks. Attackers use these SQL statements for reading, writing, and deleting operations[13]. This kind of attack can not only obtain the user's private data but also threaten the entire database system. When Web applications are attacked by SQL injection, the current page shows different outcomes compared to the true information.[5]. Recent years have seen a continuous upward trend in big internet data, and the volume of the Cloud-driven applications will only continue to grow with more individuals, governments and businesses adopting and hosting files and applications in the Cloud. A Google search of "SQLi hall of shame" throws light on how topical SQLIAs issues are.[11] SQL Injection (SQLI) is not only a vulnerability arising from developers lack of security awareness in web application development to sanitized input data, but an exploit of the free text processing capability of the SQL engine which has ramifications in both legacy and new web application lacking sanitation becoming SQLI vulnerable.[11]

The motivation behind combining IoT with data security is to secure the data which is captured by the IoT sensor at real time. For example in a power plant there are temperature and humidity sensor which collect and store the temperature data if this data is corrupted by the attacker it will affect the whole power plant.

2. SCOPE OF WORK

The analysis of SQLIA has seen numerous methodologies projected over the years by researchers. These methodologies can be categorized in to three terms.

- Firstly, SQLI Vulnerability (SQLIV) testing and detection.
- Secondly, defensive secret writing in internet application code sanitation for SQLI hindrance.
- Thirdly, dynamic runtime analysis as well as taint-based and approaches that apply AI (a similar approach enforced during this paper) within the detection and hindrance of SQLIA.

3. RELATED WORK

There are number of researches going on to detect and prevent SQL injection attacks. This research

intents to combine IoT with data security in order to secure the data which is captured by the IoT sensors at real time. Following are some techniques for detecting and preventing SQL injection attacks.

1) Numerical Encoding to Tame SQL Injection Attacks: Intruders becoming smarter in obfuscating web requests to evade detection combined with increasing volumes of web traffic from the Internet of Things (IoT), cloud-hosted and on-premise business applications have made it evident that the existing approaches of mostly static signature lack the ability to cope with novel signatures. NETSQLIA has built-in safeguards to group unrecognised patterns as unknown. It is required to exhaustively map the random decimal values attributed to variations in attack features with exploring deep ANN and ML. [1]

2) An Applied Pattern-Driven Corpus to Predictive Analytics in Mitigating SQL Injection Attack: Emerging computing relies heavily on secure backend storage for the massive size of big data originating from the Internet of Things (IoT) smart devices to the Cloud-hosted web applications. In this paper a pattern-driven data set is generated using SFA in the absence of a pre-existing data set to apply predictive analytics to SQLIA detection and prevention in a big data context. This method does not define the type of the SQL injection attack. So multi-class classifier can be used to classify different SQLIA types.[2]

3) A novel method for preventing SQL injection using SHA-1 algorithm and syntax- awareness : This method uses SHA-1 hashing function for embedded queries can add a value in performance which is critical in web applications. They proposed an algorithm that uses hash function mainly the SHA-1 to produce a new methodology for preventing SQLi in the embedded SQL queries, and also we have used syntax-awareness for protecting stored procedures from SQLi to cover as much as we can the various types of SQLi attacks. The proposed methodology can deal with login phase only or it can be used for other operations after the authentication stage.[3]

4) A Two-Tiered Defence of Techniques to Prevent SQL Injection Attacks: This technique proposes a two-tier defence technology. The first tier is the fine-grained RBAC that contains roles, activities, granular RBACSQL operations and data partitioning, the second tier is extended ACmulti-pattern matching algorithm that added to the WM pattern matching thought. The two-tiered defence that combined fine-grained RBAC with extended ACmulti-pattern matching algorithm can improve the detection efficiency and prevent the common type of SQLIA.[4]

5) AMNESIA: analysis and monitoring for NEutralizing SQL-injection attacks: AMNESIA (Analysis and Monitoring for NEutralizing SQL Injection Attacks) is the prototype tool that implements our technique to counter SQLIAs for Java-based web applications. AMNESIA is developed in Java. Queries that are not compliant with the model are identified as SQLIAs, blocked, and relevant information is reported to developers and administrators. There is a need to investigate alternate techniques for building SQL models for cases in which the static analysis cannot be used for example where the real time data is collected and stored in to the database.[5]

6) An efficient technique for preventing SQL injection attack using pattern matching algorithm: Pattern matching is a technique that can be used to identify or detect any anomaly packet from a sequential action. Injection attack is a method that can inject any kind of malicious string or anomaly string on the original string. In this research, they have proposed a scheme for detection and prevention of SQL Injection Attack using Aho–Corasick pattern matching algorithm. The proposed scheme is evaluated by using sample of well known attack patterns. So it is not efficient for novel type of attacks.[6]

7) Algorithm to prevent back end database against SQL injection attacks: In this approach the concept of ASCII values is used and at the same time made sure not a single byte of additional storage is used. Through this method it doesn't matter whatever the user has entered through the input field. The value which is matched or searched in the database will be numeric and hence there is no scope for any sort of SQL injection. The proposed scheme is evaluated by using sample of well known attack patterns. So it is not efficient for novel type of attacks.[7]

8) A Secure Coding Approach For Prevention of SQL Injection Attacks: The injection of such type of infected queries can be done by attackers through URLs or from web forms. In this research paper, a secure coding approach is proposed that can be used by web developers and security professionals to secure their application against such type of attacks at the time of coding. To check the accuracy and efficiency of proposed approach, several real time PHP based web applications have been tested and a comparison analysis is done among previous prevention techniques and proposed technique. In future, the proposed approach can be automated by developing some algorithm and real time application to facilitate web developers in more efficient manner. The whole research is done on PHP based projects, in future it can be extended to some other programming languages like Python, ASP etc.[8]

4. COMPARATIVE STUDY

Table 1. Description of different types of SQL Injection Attacks[14].

Type of attack	Attacker's aim	Description	Example
Tautologies	Bypassing authentication and extracting data	Conditional statements are formed in such a way that they are always true.	Select * from emp_info where empid=" or '7=7';
Logically Incorrect queries	To extract information about database and identify injectable patterns	Invalid queries are executed leading to error messages which constitutes information about data type or table name.	Aggregate functions applied on varchar or invalid data types Or using 'having' and 'group by' clauses.
Union Query	Bypassing authentication and extracting data	By using operator 'union', malicious query is joined with safe query.	Select * from user where user='ravi' union select * from admin where id='3142'-- 'pass='2=2';
Piggy-backed queries	Data extraction and modification, DoS	Malicious query is appended to legitimate query. On execution of first query, second also gets executed.	Select * from user where name= 'ravi' and pass='1234';drop table user;
Blind injection	-	Database schema is guessed by gathering responses on basis of true/false questions.	Attackers injects query to discover the vulnerabilities like select * from user where id='12' and pass='1=0'; to check if there is input validation or not.

Table 2.Comparison of existing methods for detecting SQL Injection Attacks.

Technique Used	Tautologies	Illegal/incorrect queries	Union queries	Piggy backed queries	Blind injection
Tautology checker	Possible	Not Possible	Not Possible	Not Possible	Not Possible
AMNESIA	Possible	Not Possible	Possible	Not Possible	Not Possible
SQL DOM	Possible	Not Possible	Possible	Not Possible	Not Possible
Prepared statements	Not Possible	Not Possible	Possible	Not Possible	Not Possible
IDS	Partially Possible	Partially Possible	Partially Possible	Partially Possible	Partially Possible

5. PROPOSED WORK

The Injector Attack Detection Tool (IDAT) tool will be tested on top of widely used applications in two scenarios, i.e. Offline Assessment and Online Evaluation. Fig 1 shows the overall work flow for SQL Injection attack detection from the IoT sensor's data.Two algorithms are developed in order to detect and prevent SQL Injection attacks.

1) Attack Client Identification Algorithm
2) Fault Injection Reduction Algorithm

The above two algorithms will detect five different types of SQL Injection Attacks. It will also classify these attacks.

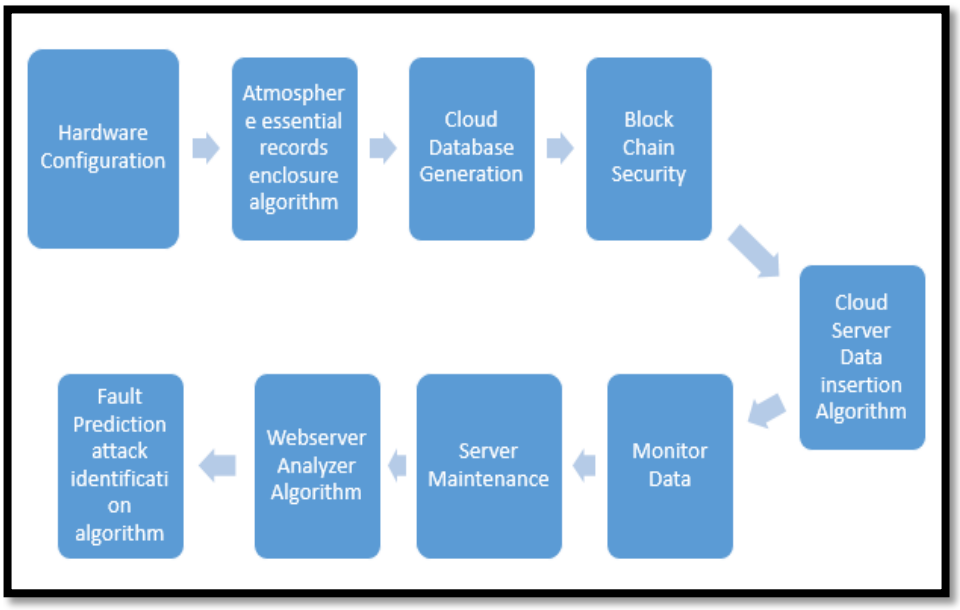

Fig. 1. Work Flow of SQL Injection attack detection system

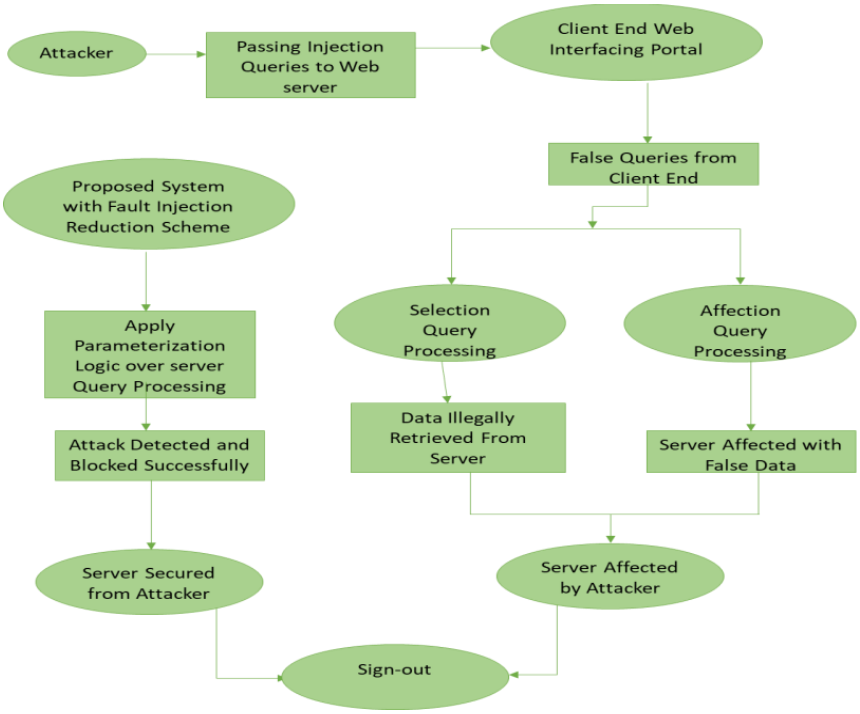

Fig. 2. Detection and prevention of SQL Injection Attack.

6. RESEARCH GAP

The existing approach regarding data security purely deals with providing complete security of private data over Web medium using attack prevention techniques. The main objective is to propose a method which can secure the intrusion inside the real-time data i.e. large amount of instantaneous data captured by the IoT sensor. In addition the existing approaches of SQL Injection attack detection only deals with the attacks which access the data. The types of SQL Injection Attacks which delete the data or manipulate the data are not detected or may be partially detected by the existing systems.

7. CONCLUSION

After the study of research papers there are various approaches to detect the SQL injection attack in web application. The research work is to detect and prevent the attack before losing any data and enhance the detection algorithm to continuously monitor real time sensor data.

REFERENCES

[1] Uwagbole, Solomon Ogbomon, William J. Buchanan, and Lu Fan. "Numerical encoding to Tame SQL injection attacks." Network Operations and Management Symposium (NOMS), 2016 IEEE/IFIP. IEEE, 2016

[2] Uwagbole, Solomon Ogbomon, William J. Buchanan, and Lu Fan. "An applied pattern-driven corpus to predictive analytics in mitigating SQL injection attack." Emerging Security Technologies (EST), 2017 Seventh International Conference on. IEEE, 2017.

[3] S. O. Uwagbole, W. J. Buchanan, and L. Fan, “Applied Machine Learning Predictive Analytics to SQL Injection Attack Detection and Prevention,” in 3rd IEEE/IFIP Workshop on Security forEmerging Distributed Network Technologies (DISSECT), 2017.

[4] Temeiza, Qais, Mohammad Temeiza, and Jamil Itmazi. "A novel method for preventing SQL injection using SHA-1 algorithm and syntax-awareness." Information and Communication Technologies for Education and Training and International Conference on Computing in Arabic (ICCA-TICET), 2017 Joint International Conference on. IEEE, 2017.

[5] Zhu, Yan, et al. "A Two-Tiered Defence of Techniques to Prevent SQL Injection Attacks." International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing. Springer, Cham, 2017.

[6] Halfond, William GJ, and Alessandro Orso. "AMNESIA: analysis and monitoring for NEutralizing SQL-injection attacks." Proceedings of the 20th IEEE/ACM international Conference on Automated software engineering. ACM, 2005.

[7] Prabakar, M. Amutha, M. Karthikeyan, and K. Marimuthu. "An efficient technique for preventing SQL injection attack using pattern matching algorithm." Emerging Trends in Computing, Communication and Nanotechnology (ICE-CCN), 2013 International Conference on. IEEE, 2013.

[8] Srivastava, Mahima. "Algorithm to prevent back end database against SQL injection attacks." Computing for Sustainable Global Development (INDIACom), 2014 International Conference on. IEEE, 2014.

[9] Gautam, Bhawana, Jyotiraditya Tripathi, and Satwinder Singh. "A Secure Coding Approach For Prevention of SQL Injection Attacks." International Journal of Applied Engineering Research 13.11 (2018): 9874-9880.

[10] Katole, Rajashree A., Swati S. Sherekar, and Vilas M. Thakare. "Detection of SQL injection attacks by removing the parameter values of SQL query." 2018 2nd International Conference on Inventive Systems and Control (ICISC). IEEE, 2018.

[11] https://codecurmudgeon.com/wp/sql-injection-hall-of-shame/

[12] https://www.smartdatacollective.com/assessing-severity-sql-injection-threats-iot-security/

[13] https://www.bitdefender.com/box/blog/smart-home/hackers-can-hit-connected-things-tricky-requests/

[14] Nagpal, Bharti, Naresh Chauhan, and Nanhay Singh. "A survey on the detection of SQL injection attacks and their countermeasures."JIPS (Journal of information Processing Systems) 2017.