2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)
December 11–12, 2019, Amity University Dubai, UAE

Impact of SQL Injection in Database Security

Himanshu Gupta
AIIT
Amity University
Noida, India
hgupta@amity.edu

Subhash Mondal
Meghnad Saha Institute of Technology
Techno India Group
Kolkata, India
Subhash@msit.edu.in

Srayan Ray
Meghnad Saha Institute of Technology
Techno India Group
Kolkata, India
contactsrayan@gmail.com

Biswajit Giri
Meghnad Saha Institute of Technology
Techno India Group
Kolkata, India
biswajitgiri.june@gmail.com

Rana Majumdar
Meghnad Saha Institute of Technology
Techno India Group
Kolkata, India
rana.majumdarwb@gmail.com

Ved P Mishra
Amity Unversity Dubai,UAE
mishra.ved@gmail.com

***Abstract*—In today's world web applications have become an instant means for information broadcasting. At present, man has become so dependent on web applications that everything is done through electronic means like e-banking, e-shopping, online payment of bills etc. Due to an unauthorized admittance might threat customer's or user's confidentiality, integrity and authority. SQL injection considered as most Spartan and dangerous coercions to the databases of web applications. In current scenario databases are highly susceptible to SQL Injection[4] . SQL Injection is one of the most popular and dangerous hacking or cracking technique . In this work authors projected a novel approach to mitigate SQL Injection Attacks in a database. We have illustrated a technique or method to prevent SQLIA by incorporating a hybrid encryption in the form of Advanced Encryption Standard (AES) and Elliptical Curve Cryptography (ECC) [5]. In this research paper an integrated approach of encryption method is followed to prevent the databases of the web applications against SQL Injection Attack. Incidentally if an invader gains access to the database, then it can cause severe damage and ends up with retrieves data or information. So to prevent these type of attacks a combined approach is projected , Advanced Encryption Standard (AES) at login phase to prevent the unauthorized access to the databases and on the other hand Elliptical Curve Cryptography (ECC) to encode the database so that without the key no one can access the database information [3]. This research paper illustrates the technique to prevent SQL Injection Attack.**

Keywords—AES, ECC, Hybrid Encryption

II. INTRODUCTION

In present scenario the usage of internet and web base services increased commendably which in turn also exploites vulnerabilities drastically [6]. SQL Injection is used by a hacker or a cracker to attack a data-driven application. This technique is used by an attacker by injecting a mischievous SQL statement during data execution for information extraction [7] purpose. Due to intrusions in current world, it is nessessary to secure the database with latest techniques[11-14]. As the proposed prevention mechanism is based on hybrid approach with a intention of to protect the database from a SQL Injection Attack [3].

A. Advanced Encryption Standard (AES)

In this approach AES parameters governed by key length, which employes the principle known as substitution-permutation network. Therefore, it is equally applicable for both software and hardware applications. Contrasting, with Data Encryption Standard (DES), Feistel network is not implemented here . The AES cipher states the number of repetitions of conversion rounds, which translate the input, say plain text, into the final output, called the cipher text [1].

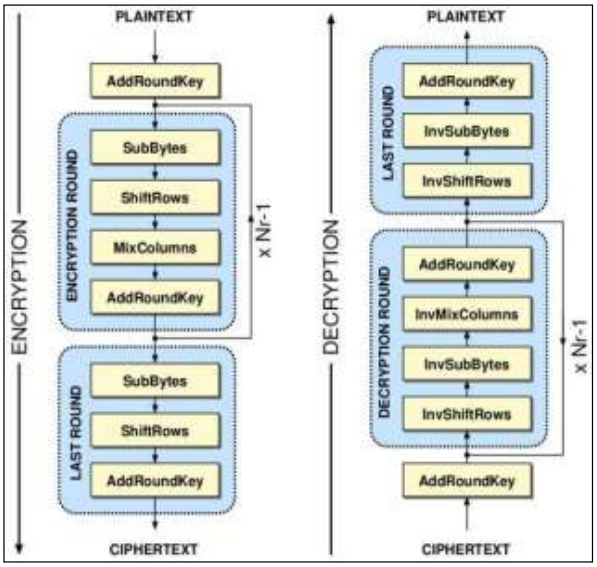

Fig. 1: Working of Advanced Encryption Standard

B. Elliptic Curve Cryptography (ECC)

Elliptical Curve Cryptography is a public-keycryptographyand is founded on the algebraic structure of elliptic curves over finite areas with smaller keys as compared to non-ECC cryptography. The this method security hinge on the skill to compute a point multiplicationand and strain of the difficulty is resoluted by the size of the elliptical curve which employs primary benefits of ECC eventually delivers the similar level of retreat by an RSA-based arrangement with a big modulus and greater key [2].

III. BACKGROUND

Over the years, many encryption techniques or methods have been developed for preventing databases from SQL injection attacks. These techniques typically follow different

978-1-7281-3778-0/19/$31.00 ©2019 IEEE

approaches. Some of the techniques are applied for such attacks are Cross-Site-Scripting (XSS) or XPath Injection [5]. On the other hand, some of the techniques were specific to some particular environment or language while others were implementation dependent.

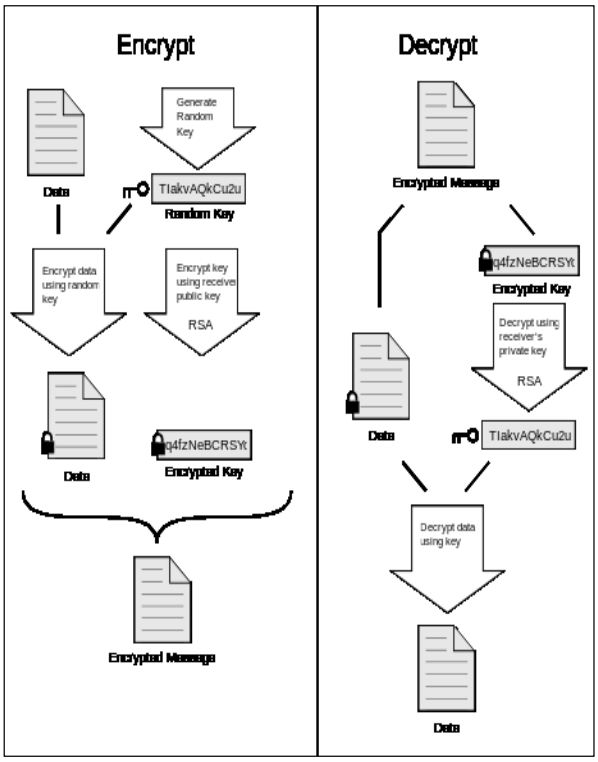

Fig. 2: Working of Elliptical Curve Cryptography

Some techniques were proposed to prevent the databases from SQL injection attack where a hybrid encryption method was applied at the login phase. There were other proposed techniques where if the SQL queries do not match with the model, then it represents a potential SQL injection attack and hence preventing execution on the databases. In this type of threat attacker alters the effect of an SQL query by introducing altered SQL keywords into the query. We have proposed a new technique for preventing the databases from the SQL injection attacks. It is more effective than the present models or techniques as we used an integrated approach towards protecting the databases against SQL injection attack. We have proposed a new technique which is based on the hybrid encryption technique. We have used Advanced Encryption Standard (AES) at the login phase for preventing unauthorized access or login to the databases and on the other hand, Elliptical Curve Encryption to encode the data stored in the database so that without the key no one can be able to access the information kept in the databank[8].

IV. PROPOSED MODEL

As stated earlier this work projected and relies on a new hybrid approach to prevent database from SQL injection outbreak. An integrated approach is employed to preventing SQL injection attack against the databases [3]. This proposed model is based on hybrid encryption technique where we have used Advanced Encryption Standard (AES) at login phase to prevent the unauthorized access to the databases and on the other hand, we have used Elliptical Curve Cryptography (ECC) to encrypt the database so that without the key no one can access the database information. During the process, two columns are created in the login table stored in the database [9]. One column is for the login id of the user and the other one is for the storage of the password. As we are using AES (Advanced Encryption Standard) we require two more columns in the login table [10]. When a user tries to login the database for the first time the login ID and the password are encrypted using Advanced Encryption Standard and the encrypted values are stored in those columns. Now whenever the user tries or desires to login to the database, it verifies the identity of the user using the username, password and the encrypted values stored in the database login table [3]. By applying encryption technique like AES, SQLIA can be detected and can prevent the database from these attacks , and encryption during login will definitely enhance security from unauthorized access.

TABLE I: LOGIN TABLE WITH SECURITY GUIDELINES AND AES VALUES

User Name	Password	Encrypted Username	Encrypted Password
Sam	12345	MH9xpxwF7KQZ1n LrDTH==	8SeBnMSLPzYgOD WbV+SdMA==
Raj	as123	y27e5ezafd2au3/2u8 XtGA==	0P14p7tmp2+sNL+i9 X46dg==

ECC is employed for encrypt the data or information stored in the databases. As the database gets encrypted by Elliptical Curve Cryptography (ECC) the user needs the correct key to access the information stored in the database[11].

In this work Elliptical Curve Cryptography is deployed to encrypt the data stored in the database. Basically ECC alters data into non readable form i.e. the data is encrypted. The main benefit of using ECC is that without the precise key, the cipher text cannot be deciphered or decrypted even if the attacker hacks the database. In this research paper combination of encryption techniques are applied in the database to protect the databases from SQL injection attacks. This is an integrated approach of encryption, which is a combination of two encryption to secure databases.

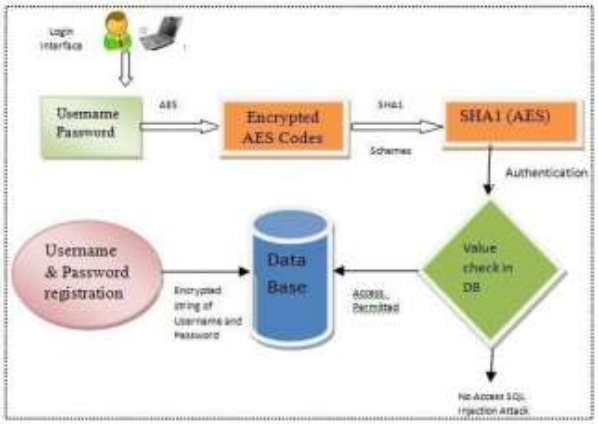

Fig. 3: Working of AES at login phase

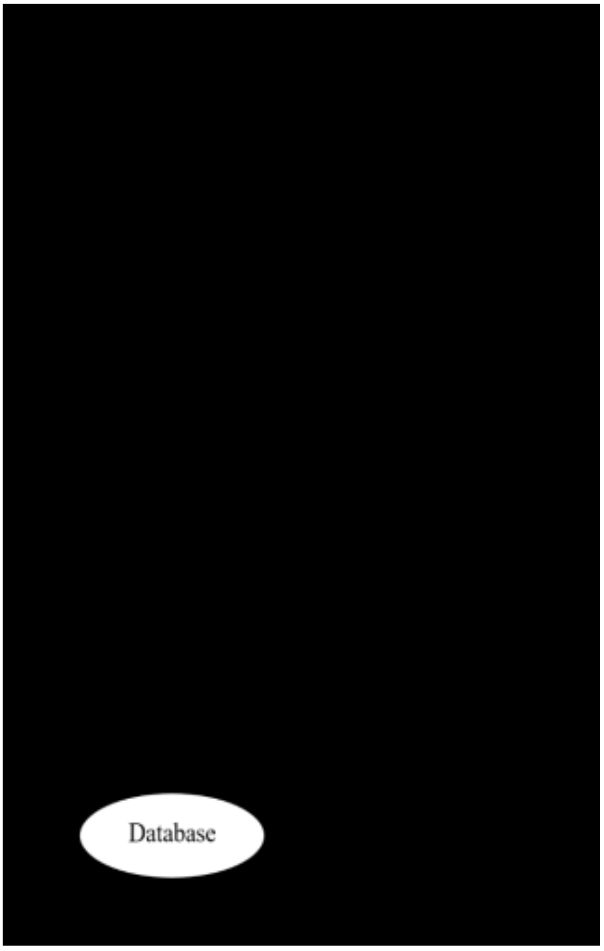

Fig. 4. Login Phase

V. Conclusion

Concluding the work with a proposed approach and its utilities in the form of protecting databases form unauthorized attacks. It is obvious that the SQL injection attacks are one of the dangerous and harmful security problem or attack. SQL injection attack is very dangerous every other type of web based application. As we have discussed above that with the increase in the use of web-applications, vulnerabilities have also increased drastically and how to combat with such difficulties by employing new approaches. Thus securing databases from the SQL injection attack.

VI. Future Work

This work focused on a particular capacity of SQL injection attack. Consequently, more research should be done in this area. With the increase of the use of web application, the SQL injection attacks will probably change and new vulnerabilities will be encountered. So to stop those attacks new countermeasures should be taken. Therefore, to prevent the future SQL injection attacks, we should do more research and find new techniques to prevent the databases from them. So in future we should try to develop a new technique which would be more capable of preventing a variety of SQL injection attacks. So the future work should be more focused on how to make this more efficient.

References

[1] What is Advanced Encryption Standard (AES)? http://searchsecurity.techtarget.com/definition/Adv anced-Encryption-Standard.

[2] What is Elliptic Curve Cryptography (ECC)? https://en.wikipedia.org/wiki/Elliptic_curve_cryptography

[3] Neha Mishra, Sunita Gond, “Defenses to Protect Against SQL Injection Attacks”, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 10, October 2013

[4] Shubham Srivastava, Rajeev Ranjan Kumar Tripathi, “Attacks Due to SQL Injection & Their Prevention Method for Web-Application”, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (2), 2012

[5] Etienne Janot, PavolZavarsky, “Preventing SQL Injections in Online Applications: Study, Recommendations and Java Solution Prototype Based on the SQL DOM”, Application Security Conference, 19th-22nd May, Belgium

[6] VVSingh, KunwarKuldeep; Gupta, Himanshu, "A New Approach for the Security of VPN”, Proceeding of ACM Second International Conference on Information and Communication Technology for Competitive Strategies (ICTCS-2016), ACM and CSI Udaipur Chapter, Udaipur, India on March 4 - 5, 2016.

[7] Jebadurai, NImmanuel;Gupta, Himanshu, “Automated Verification in Cryptography System”, Proceeding of ACM Second International Conference on Information and Communication Technology for Competitive Strategies (ICTCS-2016) organized by ACM and CSI Udaipur Chapter at Hotel Inder Residency, Udaipur, India on March 4 - 5, 2016.

[8] Singh, Gurjeet; Gupta, Himanshu,“ID Based Encryption in Modern Cryptography”, Proceeding of ACM Second International Conference on Information and Communication Technology for Competitive Strategies (ICTCS-2016), ACM and CSI Udaipur Chapter, Udaipur, India on March 4 - 5, 2016.

[9] Kumar, Sunil; Gupta, Himanshu, “Agent based Security Model for Cloud Big Data”, Proceeding of ACM Second International Conference on Information and Communication Technology for Competitive Strategies (ICTCS-2016), ACM and CSI Udaipur Chapter, Udaipur, India on March 4 - 5, 2016.

[10] Gupta, Himanshu; Sharma, Vinod Kumar; "Role of Multiple Encryption in Secure Electronic Transaction", International Journal of Network Security & Its Applications, Nov 2011.

[11] Gupta, Himanshu; Sharma, Vinod Kumar; "Multiphase Encryption: A New Concept in Modern Cryptography", International Journal of Computer Theory and Engineering, Aug 2013.

[12] Prakhar Kaushik ; Rana Majumdar , “Timing attack analysis on AES on modern processors”, 6th International Conference on Reliability, Infocom Technologies and Optimization DOI: 10.1109/ICRITO.2017.8342471 , pp. 462-465, 2017.

[13] Mishra, Ved Prakash, Balvinder Shukla, and Abhay Bansal. "Monitoring of Network to Analyze the Traffic and Analysis of Audit

Trails Using Process Mining." In International Conference on Futuristic Trends in Network and Communication Technologies, pp. 441-451. Springer, Singapore, 2018.

[14] Mishra, V.P., Dsouza, J. and Elizabeth, L., 2018, August. Analysis and Comparison of Process Mining Algorithms with Application of Process Mining in Intrusion Detection System. In 2018 7th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO) (pp. 613-617). IEEE.