An Efficient Attack Defensive Models For Web Security

Mohammad Arshad, Ali Hussain

Abstract*: *Web security plays vital role in protecting interests of genuine users associated with different web applications that are deployed in web server running either in Local Area Network (LAN) or Wireless Local Area Network (WLAN). There are many attacks possible to violate web security. They include URL interpretation, impersonation and session hijacking to mention few. These attacks make significant damage to legitimate users. They may cause financial and other risks. The existing solutions to prevent such attacks are very useful. However, a framework that is extensible and caters to the security services required by web server is important to have sustainable and continuous effort to have countermeasures to the known attacks and also unknown attacks that may be devised by adversaries in future. Towards this end, in this paper, we proposed a framework known as Attack Detection and Prevention Framework (ADPF) with mechanisms and underlying algorithms to detect and prevent various kinds of attacks that jeopardise web security. This paper has focused on three attacks though the framework is extensible to support prevention of other attacks. They are known as URL interpretation, session hijacking and impersonation. We built a prototype framework that is deployed in web server to demonstrate proof of the concept. Our experimental results revealed that the proposed framework has high utility in preventing aforementioned attacks.

Index Terms*: *Web security, automatic vulnerability detection, URL interpretation attack, impersonation attack, session hijacking attack.

I. INTRODUCTION

Web applications deployed in web server running in LAN or WLAN may be exposed to vulnerabilities. There might be developers who are not aware of different kinds of attacks leading to violating web security. Therefore the security of web applications deployed in wireless environments especially depends on the expertise of application developers. This is an important drawback as it is not possible to expect the software engineers to have such level of acumen in making security algorithms. The existing literature found that there are many attacks that need attention. Three attacks are in the scope of this paper. They are URL interpretation, impersonation and session hijacking. Solutions to URL interpretation attacks [1], [2], session hijacking attacks [11], [13], [15] and impersonation attacks [21], [24] and [28]. In the literature it is found that there are many useful contributions towards prevention of attacks like URL interpretation, session hijacking and impersonation. However, a comprehensive framework to cater to the needs of present and future attacks is highly desired. Therefore in this paper we proposed a framework that is deployable in web server and monitors web applications to prevent various kinds of attacks. The framework is known as Attack Detection and Prevention Framework (ADPF). Our contributions in this paper are as follows.

1. We proposed a framework known as Attack Detection and Prevention Framework (ADPF) which has mechanisms to detect and prevent attacks made on web security. The scope of this paper is three attacks known as URL interpretation, session hijacking and impersonation.
2. Mechanisms are defined and algorithms are proposed to make the framework effective against the aforementioned attacks.
3. A prototype application is implemented and deployed in web server to protect other deployed web applications from these attacks. The framework is evaluated and found to have good utility in ensuring web security.

The remainder of the paper is structured as follows. Section 2 provides review of literature. Section 3 provides preliminaries to understand the attacks considered in this paper. Section 4 presents the proposed framework in detail. Section 5 presents experimental results. Section 6 concludes the paper and provides directions for future work.

II. RELATED WORK

This section provides review of literature on different kinds of attacks made on web server in LAN or WLAN. Mainly it throws light into three kinds of attacks namely URL interpretation attack, session hijacking attack and impersonation attack. URL interpretation is a kind of phishing attack as explored in [1] and [2]. Various researchers in [3], [4], [5], and [6] focuses on different kinds of interpretations of URLs in order to provide security to web applications. Attack recognition with malware analysis is made in [7] while security and privacy to web applications is explored in [8]. Path overwriting and content analysis are explored in [8] and [10].

Session hijacking and its prevention measures are explored in [11], [13], [15]

Revised Manuscript Received on June 19, 2019

Mohammad Arshad,. Research Scholar, KLEF, Guntur District, A.P., India,

Md. Ali Hussain, Professor KLEF, Guntur District, A.P.

and [20]. A methodology for detection of SQL injection attacks is made in [12] while the [14] focuses on the cross site scripting attacks and prevention measures. The concept of data hijacking and its prevention is studied in [16] while the attacking scenarios on SCADA systems are the main focus in [17] and [18]. Attacks on network layers and their countermeasures are investigated in [19]. Identity based attacks with cryptography is studied in [21]. Wi-Fi impersonation attacks [22], impersonation detection in sensor networks [24], detection of impersonation attacks using weighted feature selection methods [28] and mechanism to prevent voice impersonation attacks [30] are other important contributions towards preventing impersonation attacks. Authentication schemes are explored as general security mechanisms in [23], [25], [26], [27] and [29].

In the literature it is found that there are many useful contributions towards prevention of attacks like URL interpretation, session hijacking and impersonation. However, a comprehensive framework that is extensible and caters to the needs of present and future defence against web security vulnerabilities is found to be desired. Therefore, the objective of this paper is to propose and implement an extensible framework for attack detection and prevention to ensure web security.

III. PRELIMINARIES

This section provides description of the three attacks considered in this paper. They are known as URL interpretation, session hijacking and impersonation. These attacks are analyzed and counter measures are provided in this paper in the context of web security for the application deployed in local (LAN) or Wireless LAN (WLAN) or remote web server (WAN). As wireless networks are used widely in different domains like education, information technology, entertainment and other commercial applications, there is importance to secure them. In this context, there is week security in case of wireless networks. Thus web security is under threat. The following sub sections provide information on the aforementioned attacks.

A. URL Interpretation Attack

It is the attack in which attackers alter the URL to achieve their objectives of deceiving web server and gain access to certain web applications for monetary and other gains. Every URL has protocol information, port number and certain parameters. When the parameters are altered, it can cause potential risk to the web security. By interpreting URLs differently, the adversaries try to achieve their goals.

B. Session Hijacking Attack

Session is the duration in which the web server is capable of remembering user identity and conversation. The web server is able to identify a user after authentication using the session ID. Therefore web server creates unique session id for each user who has been authenticated and sends session id to client. This session id is to be used by client with further communications so as to help the server to identify the client. When the attackers are able to steal the session ID, they are able to hijack sessions of legitimate users and perform their intended operations. This causes potential risk to genuine users.

C. Impersonation Attack

It is an attack made by adversaries to perform activities on behalf of other users. It is also known as IP spoofing attack. Such attacks exploit vulnerabilities of authentication protocols and gain access to legitimate data of users. Special IP packets are created by hackers to inject IP addresses that are not genuine and gain entry to the application running in web server.

IV. PROPOSED FRAMEWORK FOR WEB SECURITY

We proposed and implemented a framework named Attack Detection and Prevention Framework (ADPF) for web security. The framework resides in web server and communicates with web components like Servlets and JSP pages in order to detect security vulnerabilities and prevent them. There are many attacks that breach web security. In this paper we focused on three important vulnerability attacks known as session hijacking, impersonation and URL interpretation. The framework is in the middle tier in the three tier architecture. Browser is the presentation tier. Web server forms web tier while database server forms data tier. The attacks are possible with the web tier. Therefore the proposed framework runs in the web tier. The framework is extensible as it can be improved further to handle other vulnerabilities in future. The overview of the proposed framework for web security is shown in Figure 1.

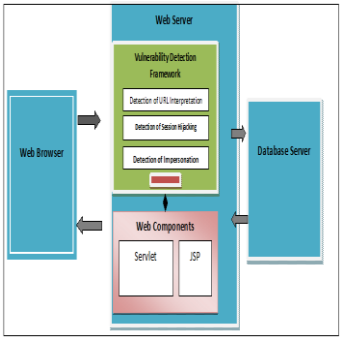

Figure 1: Proposed Attack Detection and Prevention Framework (ADPF) for web security

Every request provided by web browser goes to web server. Attackers may follow this approach or may invoke web server directly to launch attacks. When attacks are launched in either way, there needs to be protection against vulnerabilities so as to protect web applications. Web applications are deployed in the form of .WAR archives into web server. The applications run in web

container. Web container is responsible to create web components, manage life cycle of web components and create other objects like request, response, session, servlet config and servlet context. Out of all the objects, session is an important object that holds identity and conversation of a single user. It does mean that session object is created for each and every user. It may be subjected to session hijacking attack that has potential financial and other risks as adversaries can simply use the session to perform their intended activities as if done by a legitimate user. There is possibility of launching impersonation attack and URL interpretation attack. The framework proposed and implemented at server side deals with these attacks and prevents them. Towards this end, the framework has interaction with web container either directly or indirectly besides web components like Servlets and JSP pages that are server side Java technologies. The requests made by web browser are actually processed by Servlets and JSP pages. In turn these web components interact with database server in order to have the dynamism and interaction and provide dynamic responses to end users. Legitimate requests are processed as per the general approach followed in a three tier application. However, when there are suspected attacks, the proposed framework comes into picture and takes care of web security by detecting and preventing attacks aforementioned.

A. Prevention of URL Interpretation

Obfuscated URLs are used by adversaries to achieve their goal. In this paper we perform six kinds of tests against URL interpretation attacks to detect and prevent such attacks. The tests include DNS test, IP address test, URL encode test, shorted URL test, whitelist and blacklist test and URL pattern matching test. The DNS test finds any kind of phishing attack or the hidden intentions of attacker. The IP address test checks whether the IP address is in blacklist to generate security alert. The URL encode test actually finds whether the attacker encoded the URL. Shorten URL detection helps in understanding the intention of attacker to make phishing attack. Whitelist and blacklist test as the name suggests finds whether the URL is in blacklist and provides timely alert. The URL pattern matching test on the other hand detects similarity between anchor and hyper texts to know malicious intentions of attacker if any.

As presented in Figure 2, the proposed framework has this URL interpretation mechanism. Analyzer is the module that checks any issues with URL submitted by the attackers or genuine users. Then if it suspects any vulnerability, it detects and prevents attack by providing timely alerts. If analyzer does not suspect URL, the URL is subjected to the six kinds of tests aforementioned and alerts are raised if there are suspected URLs.

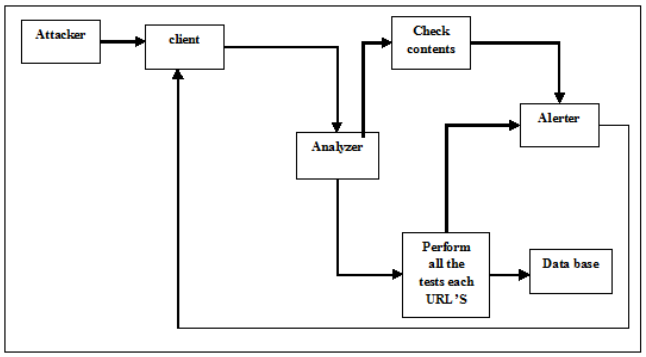

Figure 2: Detection of URL interpretation attack

B. Obfuscated URL Detection (OUD) Algorithm

This algorithm takes URLs that come to web server in any means either direct or indirect and then detects any URL interpretation attacks and prevent them. Therefore, it takes URL as input and generates alerts appropriately as output and prevents such attacks.

The proposed algorithm is simple and effective as it performs all kinds of tests to know whether there is URL interpretation attack in all the URLs that reach web server either through browser or directly from thick clients.

Algorithm 1: Obfuscated URL Detection

Inputs : URLs, whitelist W, blacklist B
Output : Alerts to prevent attack
1. Initialize URL vector
2. URL = URLs
3. For each url in URL
4. If hypertext != anchor text Then
5. Alert user
6. End If
7. If IP address not in W Then
8. Alert user
9. Add IP address to B
10. Else
11. Safe URL
12. Add IP address to W
13. End If
14. If url is found encoded Then
15. Decode URL
16. Inform user
17. End If
18. If url is found shortened Then
19. Alert user
20. End If
21. If patters in hypertext and anchor text are not matching Then
22. Alert user
23. End If

C. Prevention of Session Hijacking Attack

It is one of the "man in the middle" attacks well known to the world as it causes potential risk to genuine users. The legitimate user who has logged in already to a web server and has credentials proved to

perform various operations loses control to an attacker. Then the attacker performs illegal activities as if doing from legitimate session. We proposed an attack prevention mechanism as illustrated in Figure 3.

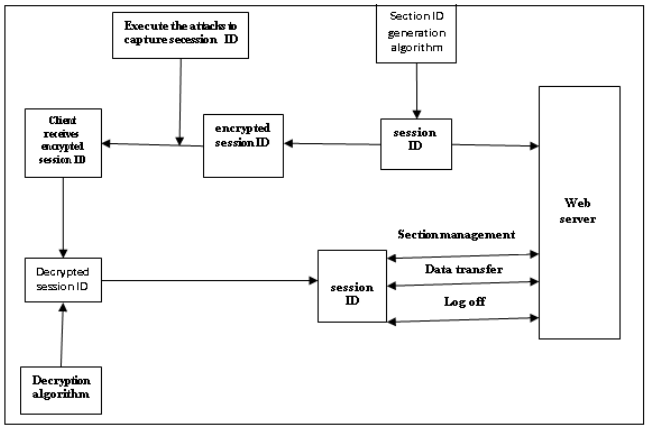

Figure 3: Mechanism to detect session hijacking attack

Before understanding the mechanism, it is important to know how sessions are created and maintained by web servers. When any user logs in, then the authenticated user will have his/her own session. It does mean that the web server creates a session object that keeps track of user's identity and conversation until he logs out. This session when hijacked, the legitimate user loses control on it while the attacker gains control over it to do his intended operations. Generally it is potential risk to genuine users in case of financial web applications pertaining to banking and other domains. As soon as session is created, the web server needs to send session ID to browser. In this process, attackers steal session ID and hijack the session. In order to prevent this kind of attack, we proposed the mechanism with encrypted session ID sent to client where decryption is made with a secret key that has been shared to client. As the session ID is encrypted, the hijackers cannot use it to have session hijacking attacks.

D. Session ID Protection (SIP) Algorithm

This algorithm is used to prevent session hijacking attacks. It follows encryption and decryption mechanisms in order to prevent capturing of original session IDs by the attackers. The securer session ID communication between browser and web server prevents this attack.

Algorithm 2: Session ID Protection

Input : Sessions S
Output: Protected sessions
1. After successful authentication web server creates session for client with unique session ID
   In case of New Sessions
2. For each session s in S
3. Session ID is encrypted and sent to client
4. Client decrypts session ID using shared secret key
5. Client sends URL along with session ID to web server
6. Web server matches session ID with available sessions
7. If session ID found Then
8. Server tracks identity of client
9. Server tracks conversation with client
10. End If
11. If session ID not found Then
12. Server does not recognize client
13. Server prevents any operations to be performed
14. End If
15. End For
    In Case of Existing Sessions
16. For each session s in S
17. Client sends URL along with session ID that has been decrypted to web server
18. If session ID not found Then
19. Server does not recognize client
20. Server prevents any operations to be performed
21. End If
22. End For

The algorithm is able to protect new and existing sessions. Only the clients that have been authenticated by web server are able to get session ID in encrypted format. The encryption and decryption mechanisms are able to protect sessions from session hijacking attacks.

V. EXPERIMENTAL RESULTS

Experiments are made with the proposed framework. The framework and a web application known as LMS (Library Management System) are deployed into Tomcat web server. Database used is MY SQL. The implementation is done using Java language. Technologies used are Servlets and JSP at server side. The security results are evaluated with the confusion matrix shown in Table 1. The results of the proposed methodology are cross validated with standard measures such as precision and recall. These are statistical measures that reflect the accuracy of the proposed algorithm in the detection of attacks.

Program	Really detected	Really not detected
Detected as per program	True Positive (TP)	False Positive (FP)
Not detected as per program	False Negative (FN)	True Negative (TN)

Table 1: Confusion matrix used for evaluation

From the confusion matrix the metrics like precision, recall and F-measure are derived as follows.

$$\text{Precision} = \frac{\text{number of true positives}}{\text{number of true positives} + \text{false positives}} \quad \ldots\ldots\ldots\ldots(1)$$

$$\text{Recall} = \frac{\text{number of true positives}}{\text{number of true positives} + \text{false negatives}} \quad \ldots\ldots\ldots\ldots..(2)$$

$$F - Mesaure = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad \ldots\ldots\ldots\ldots\ldots(3)$$

Table 2: Results of precision and recall

Attack	Precision	Recall
URL Interpretation Attack	0.98	0.6
Session Hijacking Attack	1	1
Impersonation Attack	0.89	0.92

As shown in Table 2, the results of experiments are presented in terms of precision and recall against different attacks explored.

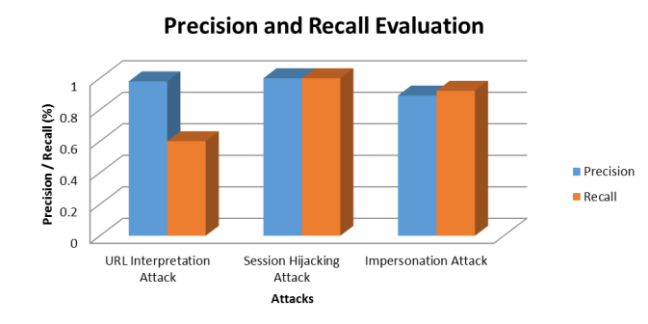

Figure 5: Results of evaluation of the ADPF

As presented in Figure 5, it is evident that the proposed framework is capable of detecting and preventing the three kinds of attacks known as URL interpretation, session hijacking and impersonation. The results revealed that the three mechanisms employed by the framework to detect and prevent attacks and ensure web security.

VI. CONCLUSION

In this paper we studied security vulnerabilities that result in attacks leading to web security problems. Various attacks are found in the literature including counter measures. The individual solutions to various kinds of attacks may help in preventing particular attacks. However, a framework that resides in web server for detection and prevention of all possible attacks is highly desired. Moreover that framework should be extensible to be futuristic. In this paper we proposed an extensible framework known as Attack Detection and Prevention Framework (ADPF) for web security. It can detect all kinds of attacks and prevent them. However, three attacks are considered in the scope of this paper. They are known as URL interpretation, session hijacking and impersonation. The framework has detection mechanism for these attacks with underlying algorithms. We built a prototype framework and deployed in web server which works to protect all web applications from aforementioned attacks. Experimental results showed the significance of the proposed framework. In future, we intend to continue our research to enhance the framework with other attacks towards a truly futuristic framework for web security.

REFERENCES

1. Ria Sankhyan, Ankit Shetty, Lubdha Dhanopia, Chetan Kaspale, Prof. Gayatri Dantal. (2018). PDS - Phishing Detection Systems. International Research Journal of Engineering and Technology. 5 (4), p1-3.
2. Jema David Ndibwile, Youki Kadobayashi, and Doudou Fall. (2017). Phishing Attack Detection by Deceptive Login Simulation through an Android Mobile App. Asia Joint Conference on Information Securit, p2-11.
3. Mostafa A. Elgendy,Ahmed Shawish,Mahmoud I. Moussa. (2014). An Enhanced Version of the MCACC to Augment the Computing Capabilities of Mobile Devices Using Cloud Computing. International Journal of Advanced Computer Science and Applications, Special Issue on Extended Papers from Science and Information Conference 2014, p13-153.
4. Sweety R. Lodha,S. Dhande. (2014). International Journal of Advance Research in Computer Science and Management Studies. ISSN. 2 (3), p1-6.
5. Swaswati Goswami, Nazrul Hoque, Dhruba K. Bhattacharyya, Jugal Kalita. (2017). An Unsupervised Method for Detection of XSS Attack. International Journal of Network Security,. 19 (5), p1-15.
6. Leslie F. Sikos. (2017). Utilizing Multimedia Ontologies in Video Scene Interpretation via Information Fusion and Automated Reasoning. Proceedings of the Federated Conference on Computer Science and Information Systems 11, p1-8.
7. Sarah Zennou, Saumya K. Debray, Thomas Dullien, and Arun Lakhotia. (2017). Malware Analysis: From Large-Scale Data Triage to Targeted Attack Recognition . IEEE, p1-10.
8. Tyrone Grandison,Larry Koved. (2015). Security and Privacy on the Web. IEEE, p1-4.
9. Sajjad Arshad,Seyed Ali Mirheidari,Tobias Lauinger,Bruno Crispo,Engin Kirda,William Robertson. (2015). Large-Scale Analysis of Style Injection by Relative Path Overwrite. IEEE, p1-10.
10. M. ESTEVE, F. MIRÓ & A. RABASA. (2018). CLASSIFICATION OF TWEETS WITH A MIXED METHOD BASED ON PRAGMATIC CONTENT AND META-INFORMATION. Nature and Ecodynamics.13 (1), p1-11.
11. Md. Shohrab Hossain, Arnob Paul, Md. Hasanul Islam. (2018). Survey of the Protection Mechanisms to the SSL-based Session Hijacking Attacks. Network Protocols and Algorithms. 10 (1), p1-26.
12. Zainab S. Alwan, Manal F. Younis. (2017). Detection and Prevention of SQL Injection Attack. IJCSMC. 6, p5-17.
13. S.S. Manivannan,E. Sathiyamoorthy. (2017). A Prevention Model for Web Application Session Hijack Attacks in Wireless Networks Using MAC Appended Session ID. Jour of Adv Research in Dynamical & Control Systems, p1-9.
14. Shashank Gupta, B. B. Gupta. (2015). Cross-Site Scripting (XSS) attacks and defense mechanisms: classification and state-of-the-art. Int J Syst Assur Eng Manag, p1-19.
15. Pan Wang,Xuejiao Chen. (2015). Co Hijacking Monitor: Collaborative Detecting and Locating Mechanism for HTTP Spectral Hijacking. IEEE, p1-7.
16. Daojuan,Yuanfang,DianjieGuo and Guangming Yu. (2017). Privacy Leaks Through Data Hijacking Attack On Mobile System. ITM web of conference, p1-6.
17. Luís Rosa, Tiago Cruz, Paulo Simões, Edmundo Monteiro, Leonid Lev. (2017). Attacking SCADA systems. IEEE, p1-6.
18. Amit Kleinmann, Ori Amichay, Avishai Wool, David Tenenbaum, Ofer Bar and Leonid Lev. (2017). Stealthy Deception Attacks Against SCADA Systems. IEEE, p2-22.
19. Abida Aslam, Mehak Abbas, Muhammad Yasir Adnan and M. Junaid Arshad. (2017). Analysis of Network Layer Attacks and their Solutions in MANET. INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY SCIENCES AND ENGINEERING. 8 (1), p1-4.
20. Michele Bugliesi, Stefano Calzavara, Riccardo Focardi and Wilayat Khan . (2015). CookiExt Patching the Browser Against Session Hijacking Attacks. Journal of Computer Security, p1-30.
21. Ria Sankhyan, Ankit Shetty, Lubdha Dhanopia, Chetan Kaspale, Prof. Gayatri Dantal. (2018). PDS - Phishing Detection Systems. International Research Journal of Engineering and Technology. 5 (4), p1-3.

22. Jema David Ndibwile, Youki Kadobayashi, and Doudou Fall. (2017). Phishing Attack Detection by Deceptive Login Simulation through an Android Mobile App. Asia Joint Conference on Information Securit, p2-11.
23. Mostafa A. Elgendy,Ahmed Shawish,Mahmoud I. Moussa. (2014). An Enhanced Version of the MCACC to Augment the Computing Capabilities of Mobile Devices Using Cloud Computing. International Journal of Advanced Computer Science and Applications, Special Issue on Extended Papers from Science and Information Conference 2014, p13-153.
24. Sweety R. Lodha,S. Dhande. (2014). International Journal of Advance Research in Computer Science and Management Studies. ISSN. 2 (3), p1-6.
25. Swaswati Goswami, Nazrul Hoque, Dhruba K. Bhattacharyya, Jugal Kalita. (2017). An Unsupervised Method for Detection of XSS Attack. International Journal of Network Security,. 19 (5), p1-15.
26. Leslie F. Sikos. (2017). Utilizing Multimedia Ontologies in Video Scene Interpretation via Information Fusion and Automated Reasoning. Proceedings of the Federated Conference on Computer Science and Information Systems 11, p1-8.
27. Sarah Zennou, Saumya K. Debray, Thomas Dullien, and Arun Lakhotia. (2017). Malware Analysis: From Large-Scale Data Triage to Targeted Attack Recognition . IEEE, p1-10.
28. Tyrone Grandison,Larry Koved. (2015). Security and Privacy on the Web. IEEE, p1-4.
29. Sajjad Arshad,Seyed Ali Mirheidari,Tobias Lauinger,Bruno Crispo,Engin Kirda,William Robertson. (2015). Large-Scale Analysis of Style Injection by Relative Path Overwrite. IEEE, p1-10.
30. M. ESTEVE, F. MIRÓ & A. RABASA. (2018). CLASSIFICATION OF TWEETS WITH A MIXED METHOD BASED ON PRAGMATIC CONTENT AND META-INFORMATION. Nature and Ecodynamics.13 (1), p1-11.

AUTHORS PROFILE

Mohammad Arshad received the bachelor degree in Electronics and computer Engineering from Acharya Nagarjuna University, India and Master degree in Computer Science Engineering from Jawahar Lal Nehru tecnnological University, India. He is Currently Pursuing the Ph.D degree in Computer Science Engineering, from Koneru Lakshmaiah Education Foundation, India. His current research interests are computer networks ,Internet privacy, network security, and mobile network data analytics.

Dr. Mohammed Ali Hussain working as Professor in Department of Electronics and Computer Engineering, KL Deemed to be University, Guntur Dist., Andhra Pradesh, India. He has received 7 National Awards and 2 International Awards for his research contributions in various International Journals (Scopus & SCI). He is Editorial Board Member & Reviewer of various International Journals. He has published 6 patents to his credit and produced 8 PhD's under his supervision. His area of Interest includes Wireless Networks, Mobile Ad hoc Networks and Web Security. He is a member of various professional bodies FISEEE, ASDF, UACEE, IACSIT and IAENG.