ISSN : 2456 - 6411

INTERNATIONAL JOURNAL OF RESEARCH IN ENGINEERING AND APPLIED SCIENCES

VOLUME NO. 15

ISSUE NO. 3

SEPTEMBER - DECEMBER - 2025

Enriched Publications
S-9,IInd FLOOR, MLU POCKET,
MANISH ABHINAV PLAZA-II, ABOVE FEDERAL BANK,
PLOT NO-5, SECTOR -5, DWARKA, NEW DELHI, INDIA-110075,
PHONE: - + (91)-(11)-45525005

ISSN : 2456 - 6411

International Journal of Research in Engineering and Applied Sciences

Aims and Scope

The Journal of Research in Engineering and Applied Sciences is an open access peer-reviewed international forum for academicians and engineers involved in research to publish high quality and refereed papers. Papers may be theoretical (including computational), experimental or both.

Papers reporting original research or extended versions of already published conference conducted by (Meghe group of Institutions) MGI or other research papers are all welcome. Papers for publication are selected through peer review to ensure originality, relevance, and readability. The journal publishes articles primarily in the following fields of engineering and science

Editorial Board

ISSN : 2456 - 6411

Patrons

Hon. Shri Datta Meghe
Chairman, NYSS, Atray Layout, Nagpur

Hon. Shri Sagar Meghe
Secretary NYSS, Atray Layout, Nagpur

Hon. Shri Sameer Meghe
Treasurer, NYSS, Atray Layout, Nagpur

ISSN : 2456 - 6411

ISSN : 2456 - 6411

International Journal of Research in Engineering and Applied Sciences

(Volume No. 15, Issue No. 3, Sep - Dec 2025)

Contents

ISSN : 2456 - 6411

ISSN : 2456 - 6411

HANDLING VULNERABLE SCRIPT CODE IN WEB ENGINEERING

Meena Deshbhratar1*, Anurag Srivastava2
Department Of Computer Science Engineering, NRI Institute of Research & Technology, Bhopal, India

ABSTRACT

Network protection in our everyday lives is becoming increasingly critical today. Since we cannot live without the Internet, it is important to have a good and security environment for networking. Cross site scripting (XSS) does, however, attack millions of websites. We can use XSS to insert malicious scripting code into apps and then return it to the customer side. If users are using the web browser to visit the injecting place of the malicious script code, it is directly run on the customer machine. The main words of XSS are commonly found in the JavaScript browser or on the server component to filter malicious code. However, it is difficult to collect all keywords in the detecting-list in order to prevent XSS attack. However, it is possible to create various forms of malicious scripting. It is also worthwhile for more people to work on XSS and find more ways to prevent XSS attacks.

Keywords – Script Code, Vulnerability Trends, Web Engineering

INTRODUCTION:

During the last decade, the Internet has seen a huge growth of the exchange of data by many means, regardless of their distance or location, by volume, nature and channel. The internet has become in particular the main channel by which global businesses operate and are extremely successful in traditional marketing strategies. Nearly every organization today continues to expand beyond its borders; therefore, almost every human endeavour and creation takes on a critical role in the network worldwide. Web apps are one of the best ways to accomplish this vital online presence. Web applications are web technology computer programs for performing tasks on the Internet. Thus, the advent of web applications and other smart devices such as smartphones, tablets and other mobile devices has changed the medium of communication and the exchange of information among platforms. With the widespread and all-round existence of these Internet applications, app developers are forced to reconsider their development strategies and shaping their security issues to avoid targeting hackers and web assailants who are finding inadequate coding practices on the Internet daily to steal sensitive information and perpetuate the Often, with the number of web applications increasing, there are vulnerabilities and a major point of discussion in various development and security forums for web applications.

Web applications usually allow sensitive customer data (such as personal details, credit card numbers

and information from social security groups) to be collected, analysed, stored and distributed immediately and repeatedly [1]. As a consequence, web applications have become main objectives of hackers who profit from miscoding, flaws in the application code, insufficient user input permission, or failure of software developers to conform to security standards. These vulnerabilities may either be found on the server side or on the client side more dangerously. SQL injection, cross-site request forgery, information leakage, hijacking of the session and cross-site scripting are the vulnerabilities. The emphasis of this paper is on the detection of cross-site attacks. Cross-site scripting is called malicious code injection in insecure web applications to trick users and redirect them to un-trusted websites (XSS). XSS can also occur when no flaw is in the servers and database engine and is probably one of the most common web applications currently exposed which is shown in Figure 1.

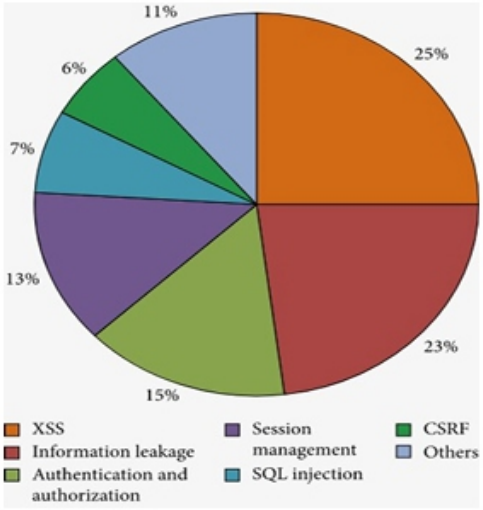

Figure 1.1Centric Application Vulnerability Trends Report

HTML types, cookies, secret fields and get and post parameters are all input sources exploited by attackers.

Three parties—the intruder and the customer—are part of the ordinary procedure. XSS violations can lead to fraud, theft of identity, regulatory penalties, loss of goodwill, litigation, and client loss.

Many research studies have focused on XSS vulnerability problem solving. In information security testing [2–4], the majority of methods cantered on preventing XSS attacks in web applications. There have been few research activities on its detection [5–6].

II. LITERATURE SURVEY

Current research aims to increase the efficiency of detection by incorporating intelligence. Current browser / device defects can be familiar (using, e.g., vulnerability bases). You can also understand how the results depend on the application's inputs. Any of these approaches are here.Cantered on model inference and evolutionary fuzzing, a novel method for detecting XSS has been developed [7]. This method simply employed a subtracting algorithm motivated by heuristics to create a crawler. They suggested an approach to infer web applications models to shape a grammar of attack. The grammar of the attack produces pieces that reduce the scope of the quest. In order to program Malicious Inputs that are sent to your application, genetic algorithms are then used. As the concept was big, it meant that the application should reset to its initial node, which may not always be useful. The frame also presumed that XSS will only be the product of one fluctuating value.

Boyer–Moore matching string algorithm was used for the detection technique in a solution proposed by Saleh et al. [8]. The characteristics of the input pattern are contrasted with the webpage characters from right to left with the heuristics referred to as the bad-type shift and the goodsuffix transition. The module's core concept is to fulfil the necessary requirements, which can search character by character for the input pattern from right to left. But the scanner takes a long time to complete its scan when the duration of the URL is long.

A working algorithm called 'NUIVT' was suggested by Abbass and Nasser[9] (novel user input validation test). There are three stages in the algorithm: The first phase analyses the fields of user input and input type detection. In the second stage input forms are transformed into regular phrases. The third phase tests are done to detect vulnerability for the invalid input, but results are from each scan to enhance the system intelligence which leads to repeat comparisons and is time consuming and tedious

Koli et al. [10] suggested SQL and XSS architecture. They have developed a SQL injection and the XSS detection method which uses HTTP request filters to look for attack signatures. To decide whether or not the script tag is present, a detection component is used. As user response, the result is stored in a database. In order to evaluate its effectiveness, they compared their work with well-known vulnerability scanners. The major downside of your research was that the tool cannot effectively detect the attack if its pattern is not stored in its database.

III. PROPOSED WORK

We propose a safe browser/ browser plug-in with its inbuilt support for JavaScript interpretation. We implement the interpreter to detect the client-side JavaScript based attacks so that the browser will not execute the unsafe statements thereby preventing the user security from getting compromised. The proposed safe browser will be able to detect various JavaScript based attacks and will not let them execute on client side. The interpreter will contain signatures of most of the well-known attacks, and it will employ regular expressions for identifying the presence of any malicious JavaScript code in the current webpage.

As an example, in cross-site scripting (XSS) attacks, a malicious web application gathers confidential data from a user. A typical example of a XSS attack is when a user is tricked into clicking on a link hosted by a malicious host (e.g., www.evil.com).

The link, appears to be pointing to a resource on a trusted site (e.g., http://www.bank.com/accounts.html, but, instead, it contains JavaScript code as the resource name. When the resource is requested by the user's browser, the code is sent as part of the HTTP request to the destination of the link (i.e., the trusted web server). Since the requested resource does not exist, the trusted web server returns an error message that contains the name of the resource that could not be accessed. As a result, the page containing the error message is interpreted by the client's browser as a page from the trusted site containing some JavaScript code. Therefore, the code is executed in the context of the trusted site and has access to the cookies previously set by the trusted site, including session identifiers and authentication tokens.

A. The Proposed Scheme

A new method for the detection and prevention of the malicious code in the scripting site is provided. The method is the combined architecture with no rules generation to detect various scripts in the database. The proposed method works as follows: Cross site scripting attacks usually taken place at the user validation or in the user input query execution.

In the proposed method the input query is clearly investigated, whether it consists of any malicious code. The following steps explains the working procedure of the method,

Classifier	Evaluation Criteria			
	Training time (sec)	Testing time (sec)	Training Accuracy (%)	Testing Accuracy (%)
Proposed Approach	0.1250	0.0313	0.7784	0.9962
ELM Kernel	0.1796	0.0065	0.7218	0.9740

Table 3.1- Comparison of proposed approach an elm-kernel

Step 1: Inputthe user Query in the available validation control.

Step 2: Identify for any script within the input entered by the user.

Step 3: Split the input values into two characters for each tag. (Eg.)

Step 4: Check the occurrence of the scripts such as Step 5: Check the given input with the predefined tags specified namely, <# …>,<=…>,

IV. RESULT AND IMPLEMENTATION

Project classification algorithms, such as the Extreme Learning Machine (ELM) and the Compare to Kernelized Extreme Learning machine were implemented (KELM). These managed algorithms for learning are carried out via MATLAB 2012. The dataset can be divided into a training set. For training purposes 80% of data was split into training data from the dataset such that 240 records out of the 300 records are included in the training data. In addition to the checked data, there are also 20% of the final data, and the test collection includes 60 records of the 300 records. In these cases, two algorithms like the Approach Proposed and the Kernelized Extreme Learning Machine (KELM) are compared according to time and precision of learning. Even if the degree of precision is closer, the time for each analysis varies. MATLAB is used to apply the Extreme Learning Machine (ELM). Here the malicious webpage has been classified by the ELM.

For the classification, the results are compared based on four factors such as training time, testing time, training accuracy and testing accuracy. There are two algorithms, for example Basic-ELM and ELM-Kernel. The analysis between 2 algorithms is shown in Table 3.1

The predictive precision shown by the Basic Proposed approach to ELM-Kernel is higher in terms of prediction accuracy, compared to the ELM kernel in the abovementioned comparative analysis (Table3.1). It takes more than the proposed approach algorithm for the model to be created via ELM-Kernel. Fig4.1 Displays the diagram of the results of the study between two algorithms

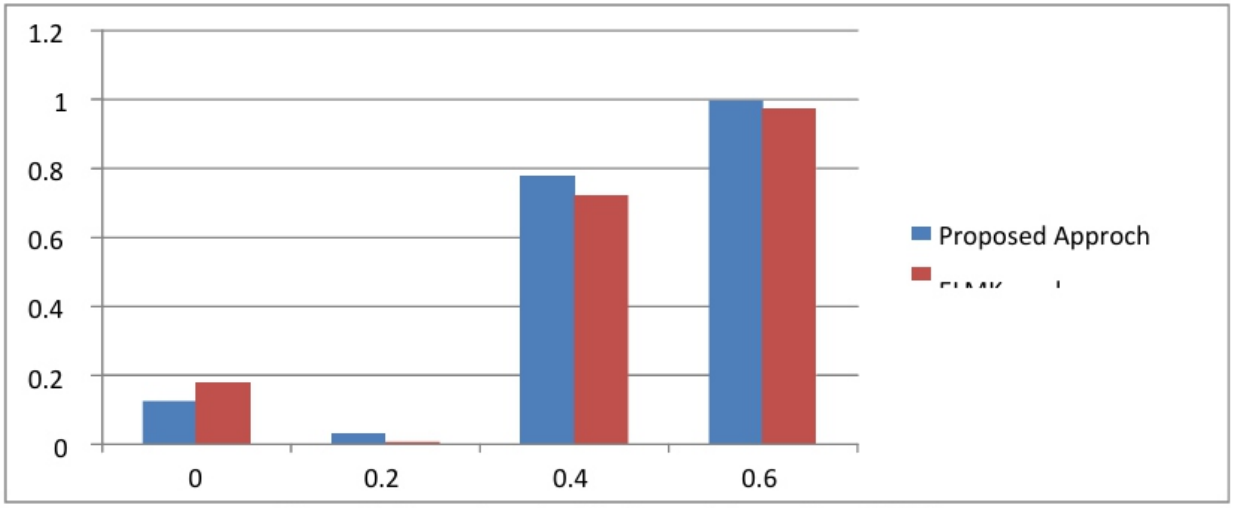

Figure 4.1: Comparison chart for Proposed Approach and KELM

V. CONCLUSION

The JavaScript language is used to boost the presentation of web pages on the client side. JavaScript is downloaded and run by an embedded interpreter in the browser onthe-fly. Browsers have sandboxing mechanisms to prevent JavaScript code from compromising the of a client environment but unfortunately there are a variety of attacks that can be used to steal user credentials, e.g. cross-site scripting attacks (e.g., phishing attacks). We suggest an approach to resolving this problem based upon browser control of the execution of JavaScript code. The trained model was created with the aid of an extreme learning machine and kernels. performance of the trained models is assessed by ten times cross validation based on prediction precision and time, and the results are analyzed. It has been observed that ELM-based prediction model shows around 99 percent predictive accuracy. For the prediction of malicious web pages, the training time and accuracy of the test play a major role in deciding the model's results. For the classifications of cross site scripting (XSS) web sites, this research work has successfully implemented Extreme Learning Machine (ELM). For the potential improvement of this study

REFERENCE

[1]H.Hibshi, Composite Security Requirements in the Presence of Uncertainty. Societal Computing Institute for Software Research, Carnegie Mellon University, Pittsburgh, PA, USA, 2016.

[2]P. Sharma, R. Johari, and S. S. Sarma, "Integrated approach to prevent SQL injection attack and reflected cross site scripting attack," International Journal of System Assurance Engineering and Management, vol. 3, no. 4, pp. 343–351, 2012.View at: Publisher Site | Google Scholar

[3]Y. Sun and D. He, "Model checking for the defence against cross-site scripting attacks," in Proceedings of the 2012 International Conference on Computer Science and Service System, pp. 2161–2164, Maui, Hawaii, January 2012.View

at: Google Scholar

[4]M. Van Gundy and H. Chen, "Noncespaces: using randomization to defeat cross-site scripting attacks," International Journal of Computer Security, vol. 31, no. 4, pp. 612–628, 2012.View at: Publisher Site | Google Scholar

[5] H. Isatou, S. Abubakr, Z. Hazura, and A. Novia, "An approach for cross site scripting detection and removal based on genetic algorithms," in Proceedings of the Ninth International Conference on Software Engineering Advances: France, pp. 227–232, Nice, France, October 2014.View at: Google Scholar

[6]P. Bathia, B. R. Beerelli, and M. Laverdière, "Assisting programmers resolving vulnerabilities in Java web applications in CCIST," Communications in Computer and Information Science, vol. 133, no. 1, pp. 268–279, 2011.View at: Publisher Site | Google Scholar

[7]F. Duchene, R. Groz, and S. A. Rwat, "Vulnerability detection using model inference assisted evolutionary fuzzing," in Proceedings of the IEEE Fifth International Conference on Software Testing, pp. 815–817, Montreal, QC, Canada, 2012.

[8] A. N. Abbass and M. Nasser, "Presentation of a pattern to counteract the attacks of XSS Malware," International Journal of Computer Applications, vol. 143, no. 2, pp. 78–88, 2016.View at: Google Scholar

[9] M. Koli, S. Pooja, H. K. Pranali, and N. G. Prathmesh, "SQL injection and XSS vulnerabilities countermeasures in web applications," International Journal on Recent and Innovation Trends in Computing and Communication, vol. 4, no. 4, pp. 692–695, 2016.

[10] M. Koli, S. Pooja, H. K. Pranali, and N. G. Prathmesh, "SQL injection and XSS vulnerabilities countermeasures in web applications," International Journal on Recent and Innovation Trends in Computing and Communication, vol. 4, no. 4, pp. 692–695, 2016

ISSN : 2456 - 6411

CONTEMPORARY SMART ANTENNA FOR MOBILE COMMUNICATION WITH ADAPTIVE BEAMFORMING ALGORITHM

Franklin Oloko1, Michael Derrek2
1,2Federal University of Uberlandia, Av. João Naves de Ávila, 2121, Santa Mônica Campus, Uberlandia, MG

ABSTRACT

The selection of smart antenna framework is a guarantee to the arrangements of the remote correspondence debilitations like wasteful use of recurrence range, week signal due to multipath engendering, and so on. The keen reception apparatus works in conjunction with advanced flag processor which is dependable to modify different parameters of the framework keeping in mind the end goal to eliminate obstruction signals and to upgrade gathering in the coveted direction(s). In this paper, an endeavor is made to create different adaptive beamforming calculations that prompt general change in the execution of the smart antenna.

Keywords- Beamforming, smart antenna, Adaptive

I. INTRODUCTION

Smart antennas otherwise called versatile exhibit radio wires, computerized reception apparatus clusters, numerous receiving wires and, as of late, MIMO) are reception apparatus clusters with savvy flag preparing calculations used to distinguish spatial flag marks, for example, the course of landing (DOA) of the flag, and utilize them to ascertain vectors which are utilized to track and find the reception apparatus shaft on the portable/target [1]. Keen receiving wires ought not be mistaken for reconfigurable reception apparatuses, which have comparable abilities yet are single component radio wires and not radio wire clusters [2].

Brilliant reception apparatus methods are utilized strikingly in acoustic flag preparing, track and sweep radar, radio space science and radio telescopes, and for the most part in cell frameworks like W-CDMA, UMTS, and LTE. Brilliant radio wires have numerous capacities: DOA estimation, beamforming, obstruction nulling, and steady modulus conservation [3].

The brilliant radio wire framework gauges the course of landing of the flag, utilizing systems, example, MUSIC (Different Flag Arrangement),estimation of flag parameters through rotational invariance strategies (ESPRIT) calculations, Lattice Pencil technique or one of their subsidiaries. They include

finding a spatial range of the receiving wire/sensor cluster, and computing the DOA from the pinnacles of this range.

Figure 1.1: Part of a series on Antennas

Smart antenna apparatus frameworks are likewise a characterizing normal for MIMO frameworks , for example, the IEEE 802.11n standard [4]. Traditionally, a smart antenna radio wire is a unit of a remote correspondence framework and performs spatial flag handling with receiving wires. Numerous radio wires can be utilized at either the transmitter or recipient.

As of late, the innovation has been reached out to utilize the various reception apparatuses at both the transmitter and beneficiary; such a framework is known as a different info numerous yield (MIMO) framework.

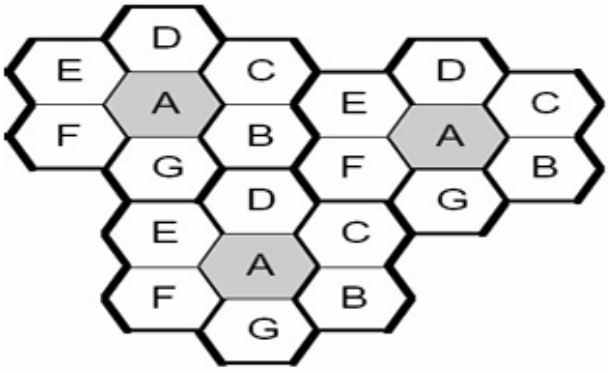

Figure 1.2: Spectrum allocation in multiple cells with frequency reuse

II. BACKGROUND

The first smart antennas were created for military correspondences and knowledge gathering. The development of cell phone in the 1980s pulled in enthusiasm for business applications [5]. The move up to advanced radio innovation in the cell phone, indoor remote system, and satellite telecom ventures made new open doors for brilliant receiving wires in the 1990s, finishing in the improvement of the MIMO (various info different yield) innovation utilized as a part of 4G remote systems [6].

These are radio wire exhibits with multi channels computerized beamforming, as a rule by utilizing FFT.

The hypothesis of the 'computerized radio wire exhibits' (DAA) began to rise as a hypothesis of multichannel estimation. Its starting points return into strategies created in the 1920s that were utilized to decide heading of the entry of radio flags by an arrangement of two receiving wires in light of the stage contrast or amplitudes of their yield voltages. In this manner, the evaluation of the headings of landing of a solitary flag was led by pointed type marker readings or as indicated by the Lissajous bends, drawn by pillar on the oscilloscope screen [7-14].

III. PROBLEM FORMULATION

Smart-antenna transceivers are substantially more unpredictable than customary base station handsets. The reception apparatus exhibit needs isolate handset chains for every radio wire component in the cluster, and precise ongoing adjustment for every one of them. In addition, the receiving wire bar shaping is computationally escalated, which implies that savvy reception apparatus base stations must be outfitted with great advanced flag processors. This tends to expand the framework costs for the time being; be that as it may, since the advantages exceed the costs, it will be less expensive over the long haul.

For a smart receiving wire to have a sensible pick up, a variety of reception apparatus components is fundamental. Subsequently, this implies a direct exhibit comprising of 10 components with a between component dividing of $\lambda/2$, working at 2 GHz, would be around 70 cm wide. This may posture issues, because of the developing open interest for less-noticeable base stations.

IV. ARCHITECTURE OF SMART ANTENNA SYSTEM

Frequency reconfigurable reception apparatuses can change progressively their recurrence of activity. They are especially valuable in circumstances where a few interchanges solitary frameworks merge in

light of the fact that the different radio wires required can be supplanted by a reconfigurable recieving wire. Recurrence reconfiguration is for the most part accomplished by adjusting physically or electrically the reception apparatus measurements utilizing RF-switches, impedance stacking or tunable materials.

Radiation pattern reconfiguration

Radiation design reconfigurability depends on the purposeful adjustment of the round appropriation of radiation design. Pillar controlling is the broadened application and comprises in guiding the bearing of greatest radiation to expand the reception apparatus pick up in a connection with cell phones. Example reconfigurable reception apparatuses are generally composed utilizing mobile/rotatable structures or including switchable and responsively stacked parasitic components.. In most recent 10 years, reconfigurable radio wires have picked up consideration due their little shape factor, wide bar directing reach and remote applications.

Polarization reconfiguration

Polarization reconfigurable recieving wires are fit for exchanging between various polarization modes. The capacity of exchanging between level, vertical and roundabout polarizations can be utilized to lessen polarization crisscross misfortunes in versatile gadgets. Polarization reconfigurability can be given by changing the harmony between the distinctive methods of multimode structure.

Compound reconfiguration

Compound reconfiguration is the ability of at the same time tuning a few reception apparatus parameters, for example recurrence and radiation design. The most widely recognized utilization of compound reconfiguration is the mix of recurrence readiness and pillar checking to give enhanced ghostly efficiencies. Compound reconfigurability is accomplished by joining in a similar structure diverse single-parameter reconfiguration procedures or by reshaping progressively a pixel surface.

V. ADAPTIVE ANTENNA APPROACH

The versatile radio wire frameworks approach correspondence between a client and base station in an unexpected way, in actuality including a measurement of room. By acclimating to a RF situation as it changes (or the spatial cause of signs), versatile radio wire innovation can progressively modify the flag

examples to close endlessness to advance the execution of the remote framework. Versatile exhibits use modern flag handling calculations to ceaselessly recognize wanted signs, multipath, and meddling signs and in ascertain their bearings of entry. This approach consistently refreshes its transmit methodology in view of changes in both the coveted and meddling sign areas. The capacity to track clients easily with primary flaps and interferers with nulls guarantees that the connection spending plan is continually augmented in light of the fact that there are neither miniaturized scale parts nor predefined designs.

Figure 5.1 shows the relative scope territory for ordinary sectorized, exchanged shaft, and versatile recieving wire frameworks . The two kinds of keen reception apparatus frameworks give critical increases over ordinary sectored frameworks. The low level of impedance on the left speaks to another remote framework with bring down infiltration levels. The huge level of impedance on the privilege speaks to either a remote framework with more clients or one utilizing more forceful recurrence reuse designs. In this situation, the obstruction dismissal capacity of the versatile framework gives fundamentally more scope than either the regular or exchanged pillar framework.

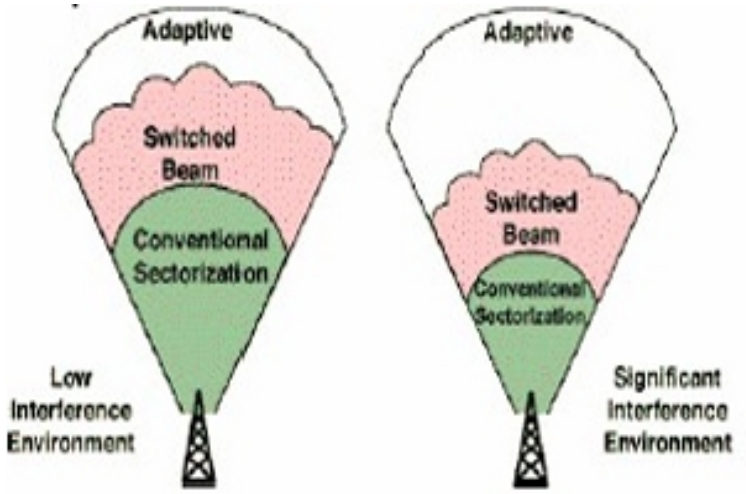

Figure 5.1: Coverage Patterns for Switched Beam and Adaptive Array Antennas

Relative Advantages/Tradeoffs of Exchanged Shaft and Versatile Exhibit Frameworks integration─ Exchanged pillar frameworks are customarily intended to retrofit generally sent cell frameworks. It has been generally actualized as an extra or appliqué innovation that brilliantly tends to requirements of develop systems. In correlation, versatile cluster frameworks have been conveyed with an all the more completely incorporated approach that offers less equipment repetition than exchanged shaft frameworks however requires new form out. extend/coverage─ Exchanged shaft frameworks can build

base station go from 20 to percent over ordinary sectored cells, contingent upon ecological conditions and the equipment/programming utilized. The additional scope can spare an administrator generous foundation expenses and means bring down costs for purchasers. Likewise, the dynamic changing from pillar to shaft monitors limit in light of the fact that the framework does not send all signs every which way. In correlation, versatile exhibit frameworks can cover a more extensive, more uniform zone with a similar power levels as an exchanged pillar framework. Exchanged pillar arrangements work best in insignificant to direct co channel impedance and experience issues in recognizing a coveted flag and an interferer. In the event that the meddling sign is at roughly the focal point of the chose shaft, and the client is far from the focal point of the chose pillar, the meddling sign can be improved significantly more than the coveted flag. In these cases, the quality is debased for the client. Versatile cluster innovation at present offers more thorough obstruction dismissal. Additionally, in light of the fact that it transmits a vast, as opposed to limited, number of mixes, its smaller concentration makes less impedance to neighboring clients than an exchanged bar approach.

Fig.5.2: Beam forming Lobes and Nulls that Switched Beam (Red) and Adaptive Array (Blue)

The framework switches its shaft in various ways all through space by changing the stage contrasts of the signs used to bolster the receiving wire components or got from them. At the point when the portable client enters a specific large scale part, the exchanged pillar framework chooses the miniaturized scale segment containing the most grounded flag.

spatial division numerous entrance (SDMA)— Among the most refined uses of brilliant recieving wire innovation is SDMA, which utilizes propelled preparing systems to, basically, find and track settled or portable terminals, adaptively directing transmission signals toward clients and far from interferers. This versatile exhibit innovation accomplishes prevalent levels of obstruction concealment, making

conceivable more proficient reuse of frequencies than the standard settled hexagonal reuse designs. Fundamentally, the plan can adjust the recurrence allotments to where the most clients are found.

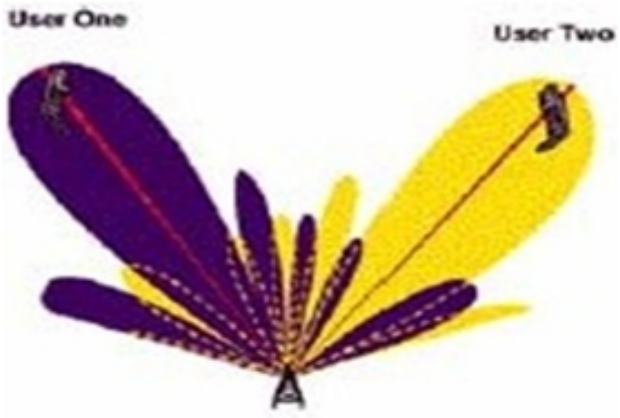

Figure 5.3: Fully Adaptive Spatial Processing, Supporting Two Users on the Same Conventional Channel Simultaneously in the Same Cell

V. RESULTS AND DISCUSSION

All through the call, the framework screens flag quality and changes to other settled smaller scale areas as required. The versatile radio wire checks its radiation design until the point when it is settled to the ideal course (toward which the flag tocommotion proportion is augmented). Toward this path the most extreme of the example is in a perfect world toward the coveted flag. Savvy radio wires comprise of in excess of a reception apparatus.

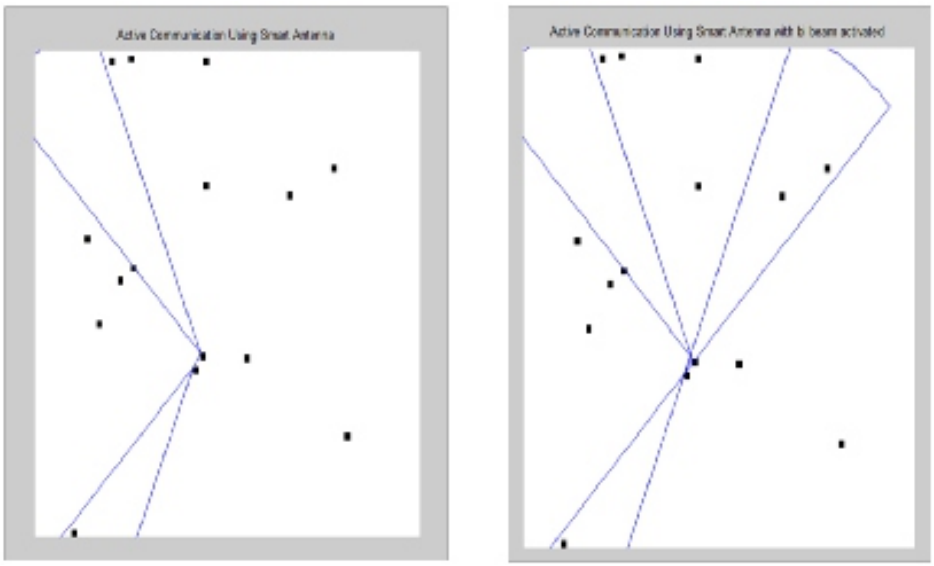

Figure 5.4: Active communication using smart antenna and bi beam activated

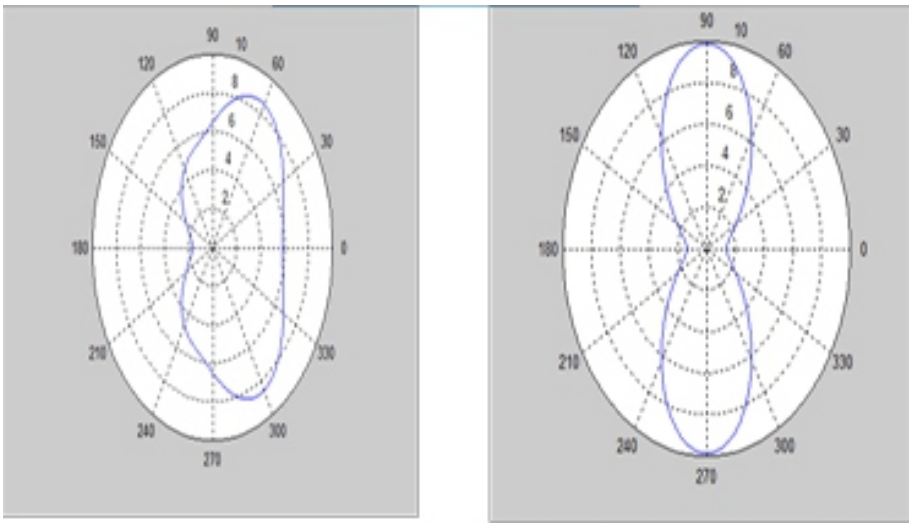

Figure 5.5: Plot of The Output Polar And Space Radiation Pattern

The radiation example of a reception apparatus is a plot of the relative field quality of the radio waves discharged by the receiving wire at various points. It is ordinarily spoken to by a three-dimensional chart, or polar plots of the level and vertical cross areas. The example of a perfect isotropic receiving wire, which transmits similarly every which way, would resemble a circle. Numerous non directional radio wires, for example, monopoles and dipoles, emanate square with control in every single flat course, with the power dropping off at higher and bring down edges; this is called an omnidirectional example and when plotted resembles a torus or doughnut.

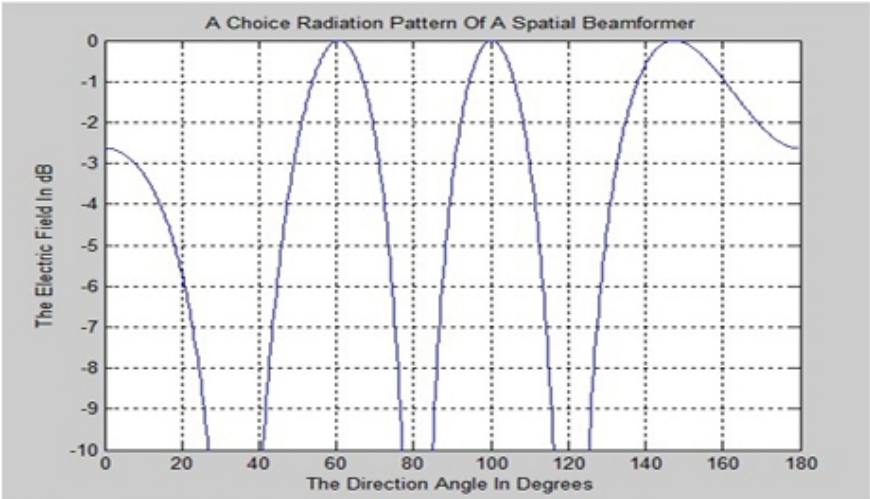

Figure 5.6: Radiation Pattern of a spatial beamformer

RREFERENCES

Ramakrishna et.al, "Hybrid Adaptive Beamforming Algorithms or Smart Antennas" IEEE 2017.

Karl Ferdinand (11 December 1909). "Nobel Lecture: Electrical Oscillations and Wireless

Telegraphy". Nobelprize.org. Nobel Media AB 2013. Retrieved 21 Oct 2013.

History of Phased Array Antennas". In Sarkar, Tapan K.; et al. History of Wireless. John Wiley & Sons. pp. 567–603. ISBN 9780-471-71814-7

Hugill, Peter J. (1999). Global Communications Since 1844: Geopolitics and Technology. Johns Hopkins University Press. p. 143. ISBN 0-8018-6039-3.

Douglas, Alan (1990). "The Legacies of Edwin Howard Armstrong". Proceedings of the Radio Club of America. 64 (3). Retrieved October 21, 2013.

Wilson, Robert W (1991). "Chapter 1: Discovery of the Cosmic Microwave Background". In Blanchard, Alain; et al. Physical Cosmology. Editions Frontieres. p. 3. ISBN 2-86332-094-7.

"History of Network Transmission". About.ATT.com. Retrieved 21 October 2013. "Early U.S. Navy Experimental Radars". History.Navy.Mil. Department of the Navy— Naval Historical Center. Retrieved 23 October 2013.

lark, Robert M. (2011). The Technical Collection of Intelligence. CQ Press. p. 179. ISBN 978-1-483-30495-3.

chonauer, Scott (5 February 2003). "Cold War relic 'Bull Ring' is being dismantled at Rota". Stars and Stripes. Retrieved 21 October 2013.

McAleer, Neil (2013). Sir Arthur C. Clarke: Odyssey of a Visionary: The Biography. RosettaBooks. ISBN 978-0-795-33297-5.

, Carlo (August 2012). "Evolution of AESA Radar Technology". Microwave Journal, Military Microwaves Supplement. Retrieved October 23, 2013.

Fenn, Alan J.; et al. (August 2000). "The development of phased-array radar technology". Lincoln Laboratory Journal. 12 (2). Retrieved October 23, 2013.

John Pike (6 March 2000). "AN/FPS-115 PAVE PAWS Radar". FAS.org. Federation of American Scientists. Retrieved 23 October 2013.

"Jansky, Karl ScienceWorld.Wolfram.com. (1905-1950)". Wolfram Research. Retrieved 23 October 2013.

ISSN : 2456 - 6411

Implementing End-to-End Encryption in Mobile Applications: Challenges and Solutions

Venkat Nutalapati1
Senior Android Developer and Security Specialist

A B S T R A C T

End-to-end encryption (E2EE) is a pivotal technology in ensuring the privacy and security of communications within mobile applications. By encrypting data at its origin and decrypting it only at its destination, E2EE prevents unauthorized access during transmission. However, implementing E2EE in mobile applications presents a range of challenges, including technical limitations, usability issues, compliance with regulatory standards, and potential security vulnerabilities. This paper explores these challenges in detail and proposes practical solutions to address them. Through a comprehensive review of current methodologies and case studies of prominent applications such as WhatsApp and Signal, this study aims to provide a nuanced understanding of how E2EE can be effectively integrated into mobile platforms. The paper highlights best practices for overcoming implementation obstacles and discusses future directions for enhancing mobile security through E2EE. By offering insights into both the theoretical and practical aspects of E2EE, this research contributes to the broader discourse on safeguarding user data in an increasingly digital world.

Keyword: Compliance, Cryptographic Algorithms, Data Privacy, Encryption Techniques, End-to-End Encryption,

I. INTRODUCTION

In the contemporary digital landscape, the protection of personal data and communications has become a pressing concern due to the exponential growth in data breaches and cyberattacks. As mobile applications increasingly serve as gateways for sensitive personal, financial, and professional interactions, ensuring the security of the information exchanged through these platforms is of paramount importance. End-to-end encryption (E2EE) has emerged as a critical technology in this endeavor, providing robust protection by encrypting data at its origin and decrypting it only at its final destination. This means that during its journey across networks, the data remains unintelligible to unauthorized parties, including potential attackers and even service providers who handle the transmission. E2EE not only safeguards the confidentiality and integrity of the data but also ensures that it is not altered or tampered with during transit. This level of security is essential in mitigating risks associated with data interception and unauthorized access, thereby enhancing user trust and safeguarding sensitive information from potential threats.

The necessity for end-to-end encryption (E2EE) has gained substantial traction in recent years, propelled by escalating concerns about privacy breaches and data security threats. Despite a robust theoretical understanding of E2EE's benefits, its implementation in mobile applications presents a complex array of challenges. Technically, the integration of encryption can impose significant performance overhead on mobile devices, potentially leading to slower app responsiveness and higher battery consumption. Usability concerns also arise, as encryption processes can complicate user experience by introducing additional steps or potential points of confusion. Furthermore, developers must navigate a labyrinth of regulatory frameworks across different jurisdictions, each with its own requirements and standards for data protection. Lastly, inherent vulnerabilities in encryption systems, such as those arising from implementation flaws or advances in cryptographic attacks, pose ongoing risks to the integrity of secure communication channels. Addressing these challenges requires a balanced approach that optimizes both security and user experience while ensuring compliance with legal standards.

This paper aims to dissect the multifaceted challenges associated with implementing End-to-End Encryption (E2EE) in mobile applications and to offer comprehensive insights into effective strategies for overcoming them. The objectives are threefold: first, to elucidate the fundamental principles and architecture of E2EE by thoroughly exploring its cryptographic foundations, key management protocols, and the technical mechanisms that ensure secure communication from end to end; second, to identify and analyze the key obstacles encountered during the integration of E2EE, which include not only technical hurdles such as computational overhead and performance trade-offs but also usability issues like user experience impacts and complexities in the integration process, as well as regulatory challenges related to compliance with privacy laws and data protection standards; and third, to propose practical solutions and best practices for addressing these challenges, drawing on a range of real-world case studies that highlight successful implementations and failures, as well as recent technological advancements that offer new tools and methodologies for enhancing E2EE deployment and management.

Through a structured exploration of these topics, this paper seeks to contribute to the ongoing discourse on mobile security and encryption. By examining both theoretical underpinnings and practical experiences, the study aims to equip developers, security professionals, and policymakers with valuable insights into implementing robust end-to-end encryption solutions in mobile applications.

2. LITERATURE REVIEW

The implementation of end-to-end encryption (E2EE) in mobile applications has been the subject of considerable academic and industry research. This literature review synthesizes key findings from various studies and publications to provide a comprehensive overview of the current state of knowledge regarding E2EE. It covers theoretical foundations, implementation challenges, case studies, and advancements in the field.

Theoretical Foundations of E2EE

End-to-end encryption is grounded in established cryptographic principles. According to Diffie and Hellman (1976), public-key cryptography secure communications by allowing users to exchange encrypted messages without pre-shared secrets. Building on these principles, E2EE ensures that data is encrypted at the sender's end and decrypted only at the recipient's end, protecting it from intermediaries (Rivest et al., 1978).

In practical symmetric and asymmetric encryption methods are employed. Symmetric encryption, such as the Advanced Encryption Standard (AES), offers efficiency for encrypting large volumes of data, while asymmetric encryption, like RSA, facilitates secure key exchanges (Katz & Lindell, 2007). Combining these methods allows for both secure communication and efficient data processing (Boneh & Franklin, 2001).

Implementation Challenges

The integration of E2EE into mobile applications presents several technical challenges. A key concern is performance overhead. Studies by Bortolameotti et al. (2015) indicate that encryption processes can introduce latency and impact device performance, especially on resource-constrained mobile devices. Optimizing encryption algorithms to minimize performance impacts remains an area of active research (Khan et al., 2018).

Key management is another critical challenge. Research by Micali and Shamir (2001) emphasizes the complexity of managing cryptographic keys securely. Issues such as key generation, distribution, and storage must be handled with precision to prevent unauthorized access (Gentry, 2009). Effective key management strategies are essential for maintaining the integrity of E2EE systems (Katz & Lindell, 2007).

Usability and User Experience

Balancing security with usability is a recurring theme in the literature. According to Egelman et al. (2013), users often struggle with understanding and managing encryption features, leading to potential usability issues. Simplifying the user experience without compromising security is a key focus for researchers and developers alike. User education and intuitive design play crucial roles in overcoming these challenges (Friedman et al., 2006).

Compliance and Regulatory Issues

Compliance with data protection regulations is a significant consideration for E2EE implementation. The General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) impose stringent requirements on data protection and encryption (Regan, 2015). Studies such as those by Solove and Schwartz (2019) explore the implications of these regulations on E2EE, highlighting the need for organizations to align their encryption practices with legal standards.

Case Studies and Practical Applications

Several case studies illustrate the practical application of E2EE in mobile applications. WhatsApp, for instance, employs the Signal Protocol for end-to-end encryption, as described by Marlinspike (2016). This implementation demonstrates how E2EE can be integrated into messaging platforms to provide secure communication while addressing performance and usability challenges.

Signal, another prominent example, offers a comprehensive case study of E2EE implementation. Research by Olsson et al. (2019) highlights Signal's approach to encryption, key management, and user experience. The platform's success underscores the feasibility of E2EE in enhancing mobile application security.

Emerging Trends and Future Directions

Emerging technologies and trends are shaping the future of E2EE. Advances in quantum computing pose potential threats to traditional encryption methods, prompting research into post-quantum cryptography (Chen et al., 2016). Additionally, innovations in secure multi-party computation and homomorphic encryption offer promising avenues for enhancing data security (Gentry & Szydlo, 2006).

The literature on end-to-end encryption provides a robust foundation for understanding its theoretical underpinnings, implementation challenges, and practical applications. Ongoing research continues to address these challenges and explore new frontiers in encryption technology, contributing to the evolving landscape of mobile application security.

3. IMPORTANCE OF END-TO-END ENCRYPTION

End-to-end encryption (E2EE) plays a crucial role in modern digital security, particularly in protecting user data within mobile applications. Its significance can be understood through the following key aspects:

Privacy Protection

E2EE ensures that only the intended recipients of a communication can access its contents. By encrypting data from the moment it leaves the sender's device until it reaches the recipient's device, E2EE prevents intermediaries, including service providers, hackers, and other unauthorized entities, from deciphering the information. This level of privacy is essential for maintaining user trust and confidentiality, especially in contexts involving sensitive or personal information.

Security Against Interception

In an era where data breaches and cyber-attacks are prevalent, E2EE provides a robust defense against interception. Without E2EE, data transmitted over networks can be intercepted and read by malicious actors. E2EE mitigates this risk by ensuring that intercepted data remains encrypted and thus unreadable without the appropriate decryption keys. This protection is vital for secure communication and transactions, such as online banking and confidential messaging.

Mitigation of Data Breach Risks

Even if a service provider's servers are compromised, E2EE ensures that the data remains protected. Since data is encrypted on the sender's device and only decrypted on the recipient's device, an attacker access to server-side data will find it inaccessible in its encrypted form. This layer of security helps in safeguarding user data against unauthorized access and potential misuse, thereby reducing the impact of data breaches.

Compliance with Data Protection Regulations With increasing regulatory requirements for data protection, E2EE can assist organizations in meeting compliance standards. Regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) mandate strict measures to protect personal data. Implementing E2EE can help organizations adhere to these regulations by ensuring that user data is encrypted and secure, thus enhancing overall compliance efforts.

User Confidence and Trust

The adoption of E2EE can significantly bolster user confidence in mobile applications. Users are more likely to trust applications that demonstrate a commitment to protecting their privacy through robust encryption practices. This trust can lead to increased user engagement, retention, and positive brand reputation, making E2EE not only a security measure but also a strategic asset for businesses.

Support for Secure Communication Channels

E2EE is foundational for various secure communication services, including messaging apps, video calls, and file sharing. By providing a secure channel for exchanging sensitive information, E2EE supports the broader goal of ensuring safe and private digital interactions. This is especially important in scenarios involving sensitive personal, financial, or health-related information.

The importance of end-to-end encryption lies in its ability to provide comprehensive privacy protection, safeguard against interception and data breaches, ensure regulatory compliance, and enhance user trust. As digital threats evolve, E2EE remains a cornerstone of effective security strategies in mobile applications and beyond.

4. KEY CHALLENGES IN IMPLEMENTING E2EE

Implementing end-to-end encryption (E2EE) in mobile applications presents several significant challenges. These challenges span technical, usability, compliance, and security domains, each of which requires careful consideration to ensure effective deployment. The following sections explore the key challenges associated with E2EE implementation:

4.1 Technical Challenges

1. Performance Impact: E2EE can introduce performance overhead due to the computational resources required for encryption and decryption processes. On mobile devices with limited processing power and battery life, the additional workload can affect application performance, leading to slower response times and increased energy consumption. Optimizing encryption algorithms and ensuring efficient resource usage are crucial to mitigating these impacts.
2. Key Management: Managing encryption keys is a complex aspect of E2EE. Keys must be securely generated, distributed, stored, and rotated. Ensuring that keys are protected from unauthorized access and misuse is essential. Additionally, handling key management efficiently in scenarios involving multiple devices or users adds to the complexity of implementation.
3. Integration with Existing Infrastructure: Integrating E2EE into existing systems and applications can be challenging. Legacy systems may not support modern encryption protocols, requiring significant modifications or upgrades. Ensuring compatibility with existing infrastructure while implementing E2EE can involve considerable effort and technical expertise.

4.2 Usability Challenges

1. **User Experience:** Balancing robust security features with a seamless user experience is a key challenge. E2EE can introduce complexities in user workflows, such as managing encryption keys or verifying secure connections. Developers must design user interfaces and experiences that are intuitive and user-friendly while maintaining strong security measures.
2. Onboarding and Education: Users may need to understand how E2EE works and how to use encryption features effectively. Providing clear guidance and educational resources is essential to help users navigate security settings and understand the implications of E2EE. Failure to educate users adequately can result in reduced effectiveness of the encryption measures.

4.3 Compliance and Regulatory Issues

1. Legal and Regulatory Requirements: Different jurisdictions have varying laws and regulations regarding data protection and encryption. Compliance with these regulations, such as the General Data Protection Regulation (GDPR) or the Health Insurance Portability and Accountability Act (HIPAA), is essential but can be complex. Organizations must ensure that their implementation of E2EE aligns with applicable legal requirements and industry standards.
2**. Impact on Law Enforcement:** E2EE can complicate lawful data access for law enforcement

agencies. While encryption is crucial for protecting user privacy, it can also hinder investigations and evidence collection. Balancing the needs for privacy and security with law enforcement requirements is a challenging issue that requires careful consideration and potential policy solutions.

4.4 Vulnerabilities and Threats

1. Potential Attack Vectors: While E2EE provides strong protection during transmission, it is not immune to vulnerabilities. Potential attack vectors include man-in-the-middle attacks during the initial key exchange, device compromise, exploitation of weaknesses in encryption algorithms. Regular updates and rigorous security practices are necessary to address and mitigate these risks.

2. Key Exposure and Misuse: The security of E2EE relies on the protection of encryption keys. If keys are exposed or compromised, the entire encryption scheme can be undermined. Ensuring that keys are securely stored and managed, and that appropriate measures are in place to detect and respond to key-related issues, is critical for maintaining the integrity of E2EE.

Implementing end-to-end encryption in mobile applications involves navigating a range of technical, compliance, and security challenges. Addressing these challenges requires a approach, combining effective technical solutions with thoughtful user experience design and adherence to regulatory requirements. By tackling these issues, organizations can successfully integrate E2EE and enhance the security and privacy of their mobile applications.

5. CONCLUSION

End-to-end encryption (E2EE) is a fundamental element of modern data security, providing strong safeguards for sensitive information in mobile applications by ensuring that data is encrypted from the point of origin to the destination, with no intermediaries able to access it. This paper delves into the multifaceted challenges associated with the implementation of E2EE. These challenges encompass technical performance impacts such as potential latency and resource consumption, which can affect application speed and efficiency. Key management complexities arise from the need to securely generate, store, and distribute encryption keys, which must be handled with meticulous care to prevent unauthorized access. Usability issues may include user experience difficulties related to managing encryption settings or recovering data in case of key loss.

Regulatory compliance adds another layer of complexity, as different jurisdictions have varying requirements for data protection, and E2EE implementations must align with these regulations to avoid

legal pitfalls. Moreover, despite its strong security posture, E2EE is not immune to potential vulnerabilities, such as weaknesses in encryption algorithms or implementation flaws that could be exploited by attackers.

A comprehensive review of existing literature, case studies, and expert insights highlights that while E2EE offers significant advantages in protecting user data from unauthorized access, its effective implementation requires a balanced approach. This involves optimizing encryption processes to minimize performance degradation, improving user experience through intuitive interfaces and support systems, and ensuring strict adherence to regulatory standards.

Additionally, continuous advancements in technology necessitate ongoing research and innovation to refine E2EE techniques and address emerging threats. As the digital landscape evolves, maintaining a robust E2EE framework is crucial not only for safeguarding data integrity and privacy but also for fostering user trust in an increasingly interconnected world. This commitment to excellence in encryption practices is vital for sustaining secure communications.

REFERENCES

[1]. Gupta, R. K. (2018). "Automated Vulnerability Scanning for Mobile Applications: Challenges and Solutions." International Journal of Information Security, 17(3), 305-320. This study discusses the benefits and limitations of automated scanning tools for mobile applications and offers solutions to address common challenges.

[2]. Muthurajan V, Narayanasamy B. An Elliptic Curve Based Schnorr Cloud Security Model in Distributed Environment. TheScientificWorldJournal. 2016;201 6:4913015.

[3]. Daniel Hess, Christof Rohrig, Remote controlling of technical systems using mobile devices, in: 2009 IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, vols. 62528, IEEE, Rende, 2009, https://doi.org/10.1109/IDAACS.2009.5342900

[4]. R.S. Yashank E-Voting HyperledgerSawtooth, System Communication using & Materials (ICACCM), International Conference on 2020.

[5]. Ali M, Khan SU, Vasilakos AV. Security in cloud computing: Opportunities and challenges. Information sciences. 2015;305:35783.

[6]. B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in softwareengineering," UK: EBSE Technical Report, Keele University, 2007

[7]. Hae-Duck Jeong, Sang-Kug Ye, Jiyoung Lim, Ilsun You, Wooseok Hyun, A computer remote control

system based on speech recognition technologies of mobile devices and wireless technologies, Comput. Sci. Inf. Syst. 11 (3) (2014) 1001–1016, https://doi.org/10.2298/CSIS130915061J

[8]. Mohit P, Amin R, Karati A, Biswas G, Khan MK. A standard mutual authentication protocol for cloud computing based health care system. Journal of medical systems. 2017;41(4):50.

[9]. Y. Qin, Q.Z. Sheng, N.J. Falkner, S. Dustdar, H. Wang, A.V. Vasilakos, When things matter: a survey on data-centric Internet of things, J. Netw. Comput. Appl. 64 (2016) 137–153.

[10]. Roy S, Das AK, Chatterjee S, Kumar N, Chattopadhyay S, Rodrigues JJ. Provably secure fine-grained data access control over multiple cloud servers in mobile cloud computing healthcare applications. IEEE Transactions on Industrial Informatics. 2018;15(1):457–68.

[11]. Arbab Waheed Ahmad, Naeem Jan, Saeed Iqbal, Chankil Lee, Implementation of ZigBee-GSM based home security monitoring and remote control system, in: 2011 IEEE 54th International Midwest Symposium On Circuits And Systems (MWSCAS), 1–4, IEEE, Seoul, Korea (South), 2011, https://doi.org/10.1109/ MWSCAS.2011.6026611.

[12]. Kapoor, Singal, A Comparative Study of K-Means, K-Means++ and Fuzzy C-Means Clustering Algorithms, IEEE International Conference on Computational Intelligence & Communication Technology, 2017 (CICT), https://ieeexplore.ieee. org/document/7977272.

[13]. Wu B, Wang C, Yao H. Security analysis and secure channel-free certificateless searchable public key authenticated encryption for a cloud-based Internet of things. PloS one. 2020;15(4):e0230722.

[14]. En Qing Ji, Hai Gang Shi, Hong Yi Li, Qian Tang, Research on new remote control platform for smart home system using mobile phones, Appl. Mech. Mater. 473 (December) (2013) 267–274. https://doi.org/10.4028/www.scientific.net/AMM.473.267

ISSN : 2456 - 6411

ENHANCEMENT OF PRODUCTION BY LEAN MANUFACTURING METHOD

Vivek Vishnu1, Vineet Kumar Dwivedi2
1Research Scholar, Department of Mechanical Engineering, SAM College of Engineering & Technology, Bhopal, India
2 Asst. Professor, Department of Mechanical Engineering, SAM College of Engineering & Technology, Bhopal, India

A B S T R A C T

The thesis proposes a method for introducing lean manufacturing using string diagram in an operating CNG high pressure storage tank manufacturing job shop at Jayfe Cylinder Ltd. Haryana. By applying lean manufacturing using process layout diagram to produce part families with similar manufacturing processes and stable demand, plants expect to reduce costs and lead-times and improve quality and delivery performance. The thesis outlines a method for assessing, designing, and implementing lean manufacturing using process layout diagram, and illustrates this process with an example. A manufacturing cell that produces high pressure steel tank container for commercial & automobile customers is implemented at cylinder tank Machining Centers. The conclusion of the thesis highlights the key lessons learned from this process.

Keywords – CNG, Lean manufacturing method, High pressure tanks

Introduction

The environment in Jayfe cylinder limited Haryana, is a bit changed and different from the one in which it has succeed in the past. The turn down in auto parts spending has increased the significance of cost in a decision process which before emphasized the incorporation of state-of-the-art technology into new Automobile products.

Linking Jayfe Cylinder Group Business and Manufacturing Strategies

Jayfe cylinder Group is the leading suppliers to Maruti, Tata motors. The Jayfe cylinder manufacturing mission incorporates the planned purpose of the group as a whole:

And with that, Manufacturing's strategy mainly focuses on to fulfil consumer need, growth and best practices. And using finest practices, Manufacturing can also provide best customer satisfaction at a low

cost, producing improved business from its current customers and attracting new ones.

An interesting expression of this strategy is the way in which major functions and interaction of manufacturing centres made.

While JPM Group has created manufacturing business units in their all-manufacturing centres that is each and every centre by having functions report to the management of the business unit, Jayfe cylinder has maintain functions, operating at a Zonal level, and supporting the manufacturing centres through their representatives.

With that, Jayfe cylinder has made a matrix approach with the intent of not just holding functional knowledge, but also to eliminate the additional costs of duplicating responsibilities or management within their each and every manufacturing centre.

Understanding the nature of the product life cycle is very useful in determining the appropriate production strategy. This chapter discusses this concept in greater length by introducing the product-process matrix.

Then, it looks after the plus points and limitations of the diverse process's structures, making it simpler to show the advantages of fine manufacturing and the conditions in which its accomplishment is enviable. Then, it tells the reasons that justify the design and moving of a manufacturing cell in the Machining Center. Finally, the procedure used to introduce the cell is made.

Product-Process Matrix

The product-process matrix joins the product and process life-cycle with the intention of providing a means whether or not a firm has correctly matched its production course to the product structure.

Since conventionally the manufacturing industry has considered itself a small producer, until recently the most of its operations had choose for a supple process layout, to allow them to manage little quantities of a large variety of products. As a result, machines are divided by function to minimize machine rest time and maximize machine use in what is often called a job shop blue print.

2. Functional and Product Flow Layouts: Benefits and Limitations

The flow and detached line flow of the product-process matrix communicates to what is often known as

a functional layout or job shop. In a functional layout tool with the same function is present with each other, providing flexibility; so a wide variety of products can be manufactured at a low volume. It also allows for easy training of workers as they have the opportunity to learn from each other when they are placed side by side.

However, the functional layout has several disadvantages. For example, as the no. of products and machine type's increase, difficulty increases largely. Since the products travel a lot around the factory, lead-times are higher and it becomes hard to look after the work-in-progress. Also, dividing products before they are sent to the next step in the process increases WIP and hides problems.

So defects are found late in the process and are generally takes large cost to correct, as there is a large no. of products in pipeline that have to be scrapped. Since maximizing machine use is an important to the environment, larger batches are preferred to minimize change-over and set-up costs.

This reason of increasing machine use causes an increase in supply costs, and finished goods and perpetuates long lead times and decreasing throughput. Goldratt in his book, has warned workers from using machine use as a driving metric, but in a functional layout it is hard to resist this attraction and give in to large inefficiencies for the sake of keeping all the machines busy.

Product-flow layouts communicate to the connected line flow in the product process matrix. These layouts are used when the product volumes prove to be big enough to a dedicated line to carry a sequence of operations, that is machines located in accordance with the line of flow of the product. The advantages of this layout are the decrease of WIP as batching is removed, and no WIP is accumulated between process steps. Since waiting times are compact considerably, cycle times reduces and throughput is higher.

One of the main disadvantages of the product-flow layouts is no flexibility, as one or a small no. of products may be manufactured in one line, and accepting product changes or new products can be costly. Product-flow layouts also require high investment to purchase manufacturing handling equipment. However, when one of the parts of equipment breaks it can cause the whole line to stop.

3. Lean Manufacturing: Limitations and Benefits

Lean Manufacturing offers an opportunity to combine the efficiency of product flow layouts with the flexibility of functional layouts. In lean manufacturing, products with similar process requirements are

placed into families and manufactured in a cell consisting of functionally dissimilar machines dedicated to the production of one or more-part families. By batching similar products, the volume increases justifying the dedication of equipment.

But since this volume is justified by process and product similarity, lean manufacturing warrants much more flexibility than a pure product-flow layout. In terms of the Product-Process matrix, lean manufacturing allows movement down the vertical axis, i.e., it allows increasing the continuity of the manufacturing process flow without demanding that the products be made in large volumes.

The benefits of lean manufacturing include faster throughput times, improved product quality, lower workin-process (WIP) levels and reduced set-up times. These gains are achieved because the batch sizes can be significantly reduced. As set-up times decrease, batch size can be reduced.

Smaller the set-up time, smaller the batch size, and as a goal a batch size of one is practical when set-up time is zero. Within a cell, small batches don't travel far as machines are placed side by side, resulting in less work-in-progress, smaller lead times and much less difficulty in production scheduling and shop floor control.

Unfortunately, in a lean layout as in the product-flow layout, a machine break down may still cause a work stoppage in the cell. A different limitation of this approach is that to make sure cell productivity and low costs, a high enough volume of products must be processed within the cell so that expense of buying the equipment to each product is low. Managers, who ignore this fact when pursuing the improvements that lean manufacturing promises, may end up with lesser benefits than expected.

Cell Design and Implementation Process

Since the goal of the internship was gaining more knowledge, it was important that the method used to would satisfy both of these objectives. In the book A New American TQM, Shiba et al. refer to 2 diverse ways to effect improvement within an organization while incorporating learning the PDCA cycle that is Plan-DoCheck-Act & the CAPD cycle.

The authors explain that the PDCA cycle is most useful in continuous improvement, where the process already exists and the PDCA cycle is run over and over again to eliminate the most important problem, and further decrease the discrepancy of the process and its results.

The CAPD cycle on the other hand, is more applicable to planning situations where the target for the next planning cycle is different from the target for the previous one. The letters are transposed to highlight the control and feedback aspects of the loop and to look upon their significance in the preparation of the development process.

4. Cell Planning Phase

The successful completion of lean manufacturing in an already established production shop depends on detailed planning, involvement of employees and management, and their staunch pledge to the change. The first three steps of the design and implementation process are incorporated in this phase: assessment, design and performance analysis. By following these steps, accurate data on the current situation is gathered and used to establish a baseline, to identify the profits from lean manufacturing, and to obtain the support of management and employees.

5. Assessment

In the assessment stage, the chief goal is to collect precise data on lead-times, costs, quality, and other important metrics to get a true image of the way in which the production environment functions. Then using analysis this data is converted intos if the cell is introduced in a new facility where the main manufacturing process/layout is not yet defined. In this case, the main point of this stage is to determine whether or not the purpose of the facility and the expected product stream go with the conditions which make lean manufacturing a helpful production method. However, this thesis will limit its scope to developing an approach to lean manufacturing in already existing production environments.

When introducing lean manufacturing in a shop like the Machining Center, which has been operating as a job shop for many years, the assessment stage not only must answer the matching question. It should explain why lean manufacturing has the prospective to yield improvements over the present manufacturing process, and create support from management to carry on with the design stage. The following list shows a short summary of the main activities to be accomplished during the assessment step:

1. Answer the match question: Is the nature of the product stream (demand and process) suited for lean manufacturing?
2. Collect accurate data on current situation: Data in every part of production is useful to know the reality of the shop and how lean manufacturing has an impact on it. Data on costs, production rates,

lead-times, metrics, level of customer satisfaction, and culture of the organization should be incorporated, but by no means this is a complete list.

3. Make the case for lean manufacturing: Building on the two previous points, the advocate for lean manufacturing must put together a strong and honest case to justify build enthusiasm in the management for lean manufacturing. The honesty and potency of the case for lean manufacturing must be emphasize; introducing a new method of "doing things" is risky and involves costs.

Management must have solid reasons to justify taking then risk and making the investment to support the new approach. Given the civilization of an association, the ability to move to the next step of the planning phase depend at least to some extent on the integrity and motives powering the party advocating lean manufacturing.

If lean manufacturing is mandated by top management, production and functional personnel may comply but not commit to the change. If the idea is originated at the grassroots, i.e. from the bottom up by either production of functional workers, the advocates may not have enough access to data or trustworthiness to make an informed suggestion to get the attention of management.

If the idea is from functions sustaining production, production person may be doubtful of the motives of the function advocating the change. Obviously, the nature of the relation between the function(s) and production is very important in such case.

Lastly, if the idea comes out of the production area, it may or may not be depending upon the amount or resources required to study its validity. The evaluation step requires that the advocate has an overall, non-sponsor approach, access to data, credibility and assurance.

Regardless of who comes up with the idea for introducing lean manufacturing, it is wise for that person to decide whether or not he is the best advocate, and identify an advocate in the case that the originator is not the best choice. Otherwise, the idea may not even make it to the assessment stage.

6. Design

The aim of the design step is to find the blue print for the cell. The achievement of this step depends on involving a core of individuals who have information or have right to use information covering different parts of production and functional support. It's highly desirable that these individuals acquire authority to make decisions as representatives of their particular functions, since the cell process requires "doing

things in a new way," which always impact the way in which functions and production "do business".

The cell layout can be finalized at this point unless the cell design team decides to leave layout open for the input of the implementation team. Before implementation other issues such as supervisory roles, labor contractual needs, level of support needed from functions, etc. should be discuss and documented as a guide or as an expectation for the implementation team.

While it is good to "cover all the bases", the author believes that there is a lot of value in leaving as many degrees of freedom as possible open to the input of the implementation team, who will eventually live and work within the cell. However, any issues that can be seen as potential barriers for successful implementation or requiring extra management guidance or clarification should be addressed.

7. Design at the Machining Center

The next few sections present the cell planning phase at the Machining Center. The planning phase consisted of a six-week period during which a cell vision team worked together to create the blue print of a production machining cell at the Center.

The goal of the project was twofold: learning and improvement. The author feels that these objectives have been accomplished. The cell design and implementation process proposed in this thesis was used to implement the cell at the Machining Centre, and the Machining Centre has begun to realize the benefits expected from the cell. Following are the key learning of author from internship:

1. Do not underrate the significance of analysis: A successful execution requires deep analysis. When introducing a cell in an already existing job shop, managers may decide to rely on their own knowledge and experience rather than on data and analysis to determine part families and cell capacity. While knowledge and experience are extremely important, without analysis it is impossible to synthesize the data into useful information to support decisions. Furthermore, analysis encourages the exploration of different scenarios, and these iterations yield a more robust design

2. People make it happen: Analysis is necessary but not sufficient. Participation from people across the organization facilitates and enhances the design; and it is people that implement the design! Ensure that input from as many of those who will "work and live within the cell" is obtained prior to implementation; it will make the implementation process much smoother.

3. Break down the functional barriers: Lean manufacturing requires communication amongst and between the operators and the functional support personnel to support rapid problem solving and results.

The culture of an already existing shop may not support the kinds of interactions and relationships that support lean manufacturing. Managers should be aware that the introduction lean manufacturing can potentially require changes to the organizational culture.

REFERENCES

[1] B. Bergman and B. Klefsjö, Kvalitetfrånbehov till användning, 5th ed. Sweden: Studentlitteratur AB, 2012.

[2] J. P. Womack, D. T. Jones, and D. Roos, The Machine That Changed the World. Great Britain: Simon & Schuster UK Ltd., 2007.

[3] P. Petersson, O. Johansson, M. Broman, D. Blücher, and H. Alsterman, Lean: Göravvikelser till framgång! Sweden: Part Development, 2009.

[4] M.L. Emiliani and D.J. Stec, "Leaders lost in transformation," Leadership & Organization Develop. J. , vol. 26, no. 5, pp. 370-387, 2005.

[5] AGA Gas AB. EttavSverigesmestinnovativaföretag. AGA - [Online]. http://www.aga.se/international/web/lg/se/like3 5agase.nsf/docbyalias/aga_histor y

[6] J. Bicheno, Nyverktygslådaför Lean. Sweden: Revere, 2006.

[7] J. K. Liker, The Toyota way - 14 management principles from world's greatest manufacturer. New-York, United States of America: McGraw-Hill, 2004.

[8] P. Found and R. Harvey, "Leading the lean enterprise," Eng. Manage., vol. 17, no. 1, pp. 40-43, 2007.

[9] N. Modig and P. Åhlström, Dettaär Lean - lösningenpåeffektivitetsparadoxen. Sweden: SSE Institute for Research, 2012.

[10] P. Hines, M. Holweg, and N. Rich, "Learning to evolve - A review of contemporary lean thinking," Int. J. of Operations and Production Manage., vol. 24, no. 10, pp. 994-1011, 2004.

[11] P. Petersson, O. Johansson, M. Broman, D. Blücher, and H. Alsterman, Ledarskap: Gör till framgång! Sweden: Part Media, 2012. Lean

[12] S. Bhasin, "An appropriate change strategy for lean success," Manage. Decision, vol. 50, no. pp. 439-458, 2012. 3,

[13] M. Alvesson and S. Sveningsson, Organizationer, ledningoch processer. Sweden: Studentlitteratur AB, 2012.

[14] K. L. Sim and J. W. Rogers, "Implementing lean production systems: barriers to change," Manage. Research News, vol. 32, no. 1, pp. 37-49, 2009.

[15] J. P. Kotter, "Leading Change: Why Transformation Efforts Fail," Harvard Bus. I. Review, pp. 57-68, March-April 1995.

[16] K. Volo and S. Volo, Engage! Your Step by Step Guide to Creating a Workplace That You, Your Co-Workers, and Your Customers Love.: Life with a Fabulous View, Incorporated, 2013.

[17] K. Ruck and M. Welch, "Valuing internal communication; management and employee perspectives," Public Relations Review, vol. 38, pp. 294-302, 2012.

[18] G. Park, M. Spitzmuller, and R. P. DeShon, "Advancing Our Understanding of Team Motivation: Integrating Conceptual Approaches and Content Areas," J. of Manage., vol. 39, no. 5, pp. 1339-1379, July 2013.

[19] R. Ilies and T. A. Judge, "Goal Regulation Across Time: The Effects of Feedback and Affect," J. of Appl. Psychology, vol. 90, no. 3, pp. 453-467, 2005.

[20] M. Kaye and R. Anderson, "Continuous improvement: the ten essential criteria," Int. J. of Quality and Rel. Manage., vol. 16, no. 5, pp. 485-506, 1998.

[21] R. K. Singh, S. Kumar, A. K. Choudhury, and M. K. Tiwari, "Lean tool selection in a die casting unit: a fuzzy-based decision support heuristic," Int. J. of Production Research, vol. 44, no. 7, pp. 13991429, April 2006.

Instructions for Authors

Essentials for Publishing in this Journal

1 Submitted articles should not have been previously published or be currently under consideration for publication elsewhere.

2 Conference papers may only be submitted if the paper has been completely re-written (taken to mean more than 50%) and the author has cleared any necessary permission with the copyright owner if it has been previously copyrighted.

3 All our articles are refereed through a double-blind process.

4 All authors must declare they have read and agreed to the content of the submitted article and must sign a declaration correspond to the originality of the article.

Submission Process

All articles for this journal must be submitted using our online submissions system. http://enrichedpub.com/ . Please use the Submit Your Article link in the Author Service area.

Manuscript Guidelines

The instructions to authors about the article preparation for publication in the Manuscripts are submitted online, through the e-Ur (Electronic editing) system, developed by **Enriched Publications Pvt. Ltd**. The article should contain the abstract with keywords, introduction, body, conclusion, references and the summary in English language (without heading and subheading enumeration). The article length should not exceed 16 pages of A4 paper format.

Title

The title should be informative. It is in both Journal's and author's best interest to use terms suitable. For indexing and word search. If there are no such terms in the title, the author is strongly advised to add a subtitle. The title should be given in English as well. The titles precede the abstract and the summary in an appropriate language.

Letterhead Title

The letterhead title is given at a top of each page for easier identification of article copies in an Electronic form in particular. It contains the author's surname and first name initial .article title, journal title and collation (year, volume, and issue, first and last page). The journal and article titles can be given in a shortened form.

Author's Name

Full name(s) of author(s) should be used. It is advisable to give the middle initial. Names are given in their original form.

Contact Details

The postal address or the e-mail address of the author (usually of the first one if there are more Authors) is given in the footnote at the bottom of the first page.

Type of Articles

Classification of articles is a duty of the editorial staff and is of special importance. Referees and the members of the editorial staff, or section editors, can propose a category, but the editor-in-chief has the sole responsibility for their classification. Journal articles are classified as follows:

Scientific articles:

1. Original scientific paper (giving the previously unpublished results of the author's own research based on management methods).

2. Survey paper (giving an original, detailed and critical view of a research problem or an area to which the author has made a contribution visible through his self-citation);

3. Short or preliminary communication (original management paper of full format but of a smaller extent or of a preliminary character);

4. Scientific critique or forum (discussion on a particular scientific topic, based exclusively on management argumentation) and commentaries. Exceptionally, in particular areas, a scientific paper in the Journal can be in a form of a monograph or a critical edition of scientific data (historical, archival, lexicographic, bibliographic, data survey, etc.) which were unknown or hardly accessible for scientific research.

Professional articles:

1. Professional paper (contribution offering experience useful for improvement of professional practice but not necessarily based on scientific methods);
2. Informative contribution (editorial, commentary, etc.);
3. Review (of a book, software, case study, scientific event, etc.)

Language

The article should be in English. The grammar and style of the article should be of good quality. The systematized text should be without abbreviations (except standard ones). All measurements must be in SI units. The sequence of formulae is denoted in Arabic numerals in parentheses on the right-hand side.

Abstract and Summary

An abstract is a concise informative presentation of the article content for fast and accurate Evaluation of its relevance. It is both in the Editorial Office's and the author's best interest for an abstract to contain terms often used for indexing and article search. The abstract describes the purpose of the study and the methods, outlines the findings and state the conclusions. A 100- to 250-Word abstract should be placed between the title and the keywords with the body text to follow. Besides an abstract are advised to have a summary in English, at the end of the article, after the Reference list. The summary should be structured and long up to 1/10 of the article length (it is more extensive than the abstract).

Keywords

Keywords are terms or phrases showing adequately the article content for indexing and search purposes. They should be allocated heaving in mind widely accepted international sources (index, dictionary or thesaurus), such as the Web of Science keyword list for science in general. The higher their usage frequency is the better. Up to 10 keywords immediately follow the abstract and the summary, in respective languages.

Acknowledgements

The name and the number of the project or programmed within which the article was realized is given in a separate note at the bottom of the first page together with the name of the institution which financially supported the project or programmed.

Tables and Illustrations

All the captions should be in the original language as well as in English, together with the texts in illustrations if possible. Tables are typed in the same style as the text and are denoted by numerals at the top. Photographs and drawings, placed appropriately in the text, should be clear, precise and suitable for reproduction. Drawings should be created in Word or Corel.

Citation in the Text

Citation in the text must be uniform. When citing references in the text, use the reference number set in square brackets from the Reference list at the end of the article.

Footnotes

Footnotes are given at the bottom of the page with the text they refer to. They can contain less relevant details, additional explanations or used sources (e.g. scientific material, manuals). They cannot replace the cited literature.
The article should be accompanied with a cover letter with the information about the author(s): surname, middle initial, first name, and citizen personal number, rank, title, e-mail address, and affiliation address, home address including municipality, phone number in the office and at home (or a mobile phone number). The cover letter should state the type of the article and tell which illustrations are original and which are not.

Notes: