## Guest Editorial Preface

# Special Issue on Advance Research in Model Driven Security, Privacy, and Forensic of Smart Devices

Gulshan Shrivastava, National Institute of Technology, Patna, India
Nhu Nguyen Gia, Duy Tan University, Da Nang, Vietnam
Mohamed Salim Bouhlel, University of Sfax, Tunisia
Kavita Sharma, National Institute of Technology, Kurukshetra, India

In the past decade, privacy and forensic analysis concerns with smart devices have becoming a key research area. The smart devices provide enhanced features such as an optimized display, in-house health monitoring, people tracking, driving directions, etc. Smart device forensics analysis is a classification under digital forensics that mainly deals with the analysis of digital evidence found in smart devices such as Smartphones, tablets and Smartwatch. There is an enormous rate of increase in threats with constantly increasing releases of smart devices and hasty development of innovative technologies. Digital forensics analysis procedure to acquire and analyze digital evidence originated in a smart device based on file systems, logical memory storage and operating system architectures. The aim of this issue is to combine the various perspectives of secure integration of attributes as well as basic research in this important discipline of security and privacy. Various scholastic studies over the past decade have set up the significance of security in information management. An established security policy will help the organizations to empower better decisions.

## IN THIS ISSUE

In the first article explore the dynamics of worm propagation in Wireless Sensor Network that is based on epidemic theory. This article includes the quarantine and vaccination class with a traditional SIR model. Pre-vaccination means nodes are immunized by antivirus initially and quarantine is a process through which infectious nodes become isolated from the system. The important parameter basic reproduction number expression derived which plays an important role the study worm propagation. If its value is less than one the system will be worm free and stable otherwise worm exists in the network and unstable. For designing, the point of view discusses the communication radius of a node and the number of nodes deployed in the sensor area for seamless communication. If a radius is large, more energy is consumed and if small the number of nodes required is lessened to deploy in the sensor area. Therefore, finding the threshold value of the communication radius and node density is key. They derived the expression for communication radius and node density as well as establish the relation between the communication radius and the basic reproduction number. Through this method, the lifetime of the wireless network can be improved. The proposed model is compared with the existing model and it is proven that the proposed model is better than the existing model. The proposed model was verified with the help of a simulation.

The research focus in the second article is to present a method to prevent the misuse of personal information through a highly secured user authentication mechanism. The most basic form of user authentication is performed by providing passwords in Latin and other well-known scripts using keyboards available on smart devices. Supplying handwritten passwords in native scripts will provide enhanced security because to break such passwords the intruder not only needs to identify the native script in which the password is written but also the knowledge about that script. However, this mechanism requires the development of an efficient system to recognize the scripts, as well as the words used, as passwords and the recognition process, must be in online mode rather than offline. The proposed system for online handwritten script identification and word recognition in the four most popular Indic scripts will facilitate the prevention of hacking of secret information stored in smart devices. The proposed system will also help the users to identify different characters in the Indic scripts through the online text to speech processing.

The third article thoroughly captures and analyzes server protection and applications from hazardous DDoS attacks which is now a necessity for all the organizations that have an online presence. Botnets have eased the execution of a DDoS attack making these organizations a potential target and impacting numerous online services like trading platforms, financial services, healthcare, etc. The authors list some well-known DDoS attacks and the need for an effective mitigation system, which they present using their novel access control lists method. In addition, they propose a novel two-way methodology, which effectively curbs the attacks at the origin with the acceptance and coordinated effort of the internet service provider (ISP). This is by filtering out the attacks close to their source, reducing the load on other routers and making it better than other techniques like web referrals and linear prediction model. The hybrid mechanism eliminates the bogus traffic at the source itself and guarantees the packets with a high priority pass through the network, reaching the specified destination so that no services are denied to the clients. In addition, the authors define filtering rules which provide security by restricting a user's access to the network, therefore, limiting access to traffic into the network. The scheme is implemented using the weighted random early detection (WRED) algorithm and graphical network simulator (GNS3) experiments are conducted in a simulated test environment.

The next article proposes model-based testing, which plays an important role in the development of software. In model-based testing, we have made the use of UML activity diagrams to identify errors and bugs during the design phase of software, thus, increasing the possibility of fault detection and correction at the early stage of software development life cycle. In the proposed approach, for every smart application, UML activity diagrams are converted into a corresponding activity graph and then a depth first search algorithm was used for the generation of test paths. It is very difficult to generate test cases for each and every generated test paths. Therefore, meta heuristic algorithms were used for securing the optimisation of test paths. We have used the hybridisation of a Tabu search and a genetic algorithm for the optimisation of test paths using the case studies of Samsung Pay, online airline reservation systems, an ATM withdrawal system and a library management system. The cost value of the test path has been used as a fitness function for securing optimized test paths. The results of hybrid genetic Tabu search (HGTO) algorithm have been compared with a simple genetic algorithm using two parameters: execution time and the total number of iterations. It is found that HGTO algorithm takes less time with lower number of iterations, as compared with the simple genetic algorithm. The proposed HGTO algorithm automatically optimizes test paths with minimum time and cost thus helps the developer to improve the quality of software product by finding critical test paths before the implementation stage.

The last article examines thoroughly captures and analyzes the attack resistant and scalable pool-based key management scheme towards NGI. This article presents a detailed explanation of various threats like: repudiation, data corruption, session hijacking, wormholes, traffic analysis, a Sybil attack, an SYN flooding attack, a malicious attack, a replay attack, a sinkhole attack, a blackhole attack, a DoS attack, eavesdropping, and jamming. The authors proposed a key management scheme and evaluated for the performance metric like delay (transmission delay, processing delay, and propagation delay) and the results show that it is scalable in nature, which is prime need of NGI due to the economics of scale. The proposed key management scheme has been evaluated in two scenarios viz. centralized and decentralized and its formal security analysis also proves that it is safe from a replay attack.

Furthermore, this article also presents a comprehensive analysis of different key management scheme and the parametric evaluation of this.

We would like to thank all the authors who kindly contributed their articles for this special issue and the editor-in-chief of IJISMD for their kind help and co-operation. We are also grateful to the IGI Global editorial office and the publishing and production teams at IGI Global Group for their assistance in preparation and publication of this special issue.

*Gulshan Shrivastava*
*Nhu Nguyen Gia*
*Mohamed Salim Bouhlel*
*Kavita Sharma*
*Guest Editors*
*IJISMD*

*Kavita Sharma is working as research scholar in NIT, Kurukshetra, India. She received a MTech (Information Security) from Ambedkar Institute of Technology, New Delhi, India. She is affiliated with G.G.S. Indraprastha University after completing her Bachelor of Technology Degree in Information Technology from the I.M.S. Engineering College, Ghaziabad, India. She has written a book which is published by Suhavi Publication, India. She is also holds positions in editorial teams of various international journals and magazines of high repute. She has published more than 20 research papers in peer refereed international journals/conference She is member of the IEEE, ACM and many other professional bodies. She has participated in different national & international workshops. Her area of interest includes smartphone security, WSN, data structures and algorithms, web mining, programming languages, cryptography and data security.*