Engineering and Establishing the Secure System of Online Examination within Multi-Campus Environment using Sensor Network Technology:

Kawser Mohiuddin,
PhD Scholar, Department of Computer Science,
OPJS University Rajasthan - India.

Prof. Dr. K. P. Yadav,
Director,
KCC Institute of Technology & Management - India.

Abstract: Majority of the present days examinations are online examinations including the university examinations or any recruitment process, the online examinations are economic, faster & reliable. WSN Technology is being deployed across the globe for various operations, but in this paper we propose the use of Sensor Networks in administrating the online examination. A virtual machine operating through server monitors all the client nodes either in its network. In this paper, a simple system is proposed that provides security for improvement of on-line examination using sensor nodes and various other IT tools & techniques including biometric authentication, firewalls, cryptography, network protocols etc. A framework is also given for conducting online examination. The proposed system assures a secure cryptographic communication individually or within a group with pre-assigned static IP addresses to the group clients. It is mainly ensured that online examination must not get altered, disturbed or compromised in anyway. In this system, with unique static IP addresses, every candidate will use his username & one time password provided by the server via the exam superintend at the time of examination. In remote cases, OTP can be sent via SMS. The examination roll no's will act as candidate usernames. As the student logs in with correct username & OTP, his all details along with particular machine IP are mapped into a log file in the respective server. The encrypted answer file will not be submitted until its particular log file containing candidate's username & machine IP address is not matched & submitted first. The entire node to node and practical supervision will be done by self organized sensor nodes.

Keywords: Online Examination, Sensor Nodes, Encryption, OTP, Static IP, Biometric, Virtual Machine etc.

I. Introduction:

We must realize the mode of online examinations as an economic, faster and reliable method to evaluate a candidate's knowledge using modern computer technology without any effects on the traditional university examination that uses pens, papers and personnel for supervision. Online exam can improve the standards of student's examination whereas the traditional examination system using the pen and paper requires more effort on the part of students and invigilators. Online examinations are considered an important source for every examination, and the development of sensor network technology polices has given the possibility to monitor the online exams perfectly. The online process using sensor nodes helps the removal proxies and cheating in examination area. This paper proposes the usage of sensor nodes and biometrics which supports the monitoring and security control, authentication and integrity of online examinations. This paper provides the solution for online examination of students at particular locations at a same time. Considering the examination of 500 students in five different buildings. We may require a minimum of 20 biometric devices and 50 sensor nodes. Biometric devices will be used at entry points for recognizing the fingerprint of the candidate. This will be matched with the server record taken earlier during admissions. The candidates enrollment number will be generated and can be used as username only after his fingerprints are matched and accepted by server,

otherwise a candidate will not be able to logon. The sensor nodes will continuously monitor the student location in beginning and will ensure the student is sitting on the right place assigned to him as per the enrollment sequence or gender sequence. Secondly the sensor nodes will monitor their assigned 10 students only and will transmit the live data to server. For 500 students we have used 50 cameras by creating the virtual partition of entire examination area into 50 partitions containing 10 students respectively. The students will not be aware of these virtual partitions. Their voice and moments will be continuously monitored and transmitted to the supervision team in server room. Any student violating the norms will not only loose the examination but will get disqualified also. His enrollment number will get hot listed and also his answer script will not be fetched by server at end. However each and every student will have an on-demand communication access to the supervision team. Once the examination is over, the answer scripts from all the client machines except hot listed ones will be fetched into server for further processing and award preparations. The sensor nodes are not helpful only in theoretical examinations, but are more productive in conducting field and practical examination in open fields, forests, deserts, crowds or mountains etc. The WSN Technology (Wireless Sensor Networks) is composed of unique devices known as nodes that have ability to sense the environment and communicate the sensed information gathered from the monitored field to the base through wireless networks. The sensed information is routed to the base through multiple hops. The base station can use it locally or is broadcasted to other networks including internet through gateways. The sensor nodes can be mobile or immobile. They may be conscious or unknowing about their locations [1]. The applications of Sensor Networks to the world is unlimited, from environmental monitoring, health care, intrusion detection, temperature & humidity reporting, positioning and target tracking, localization, and so on. Wireless sensor networks are composed of a large number of wirelessly communicating and computing devices, nodes.

II. Securing the Examination Resources and Environment:

Secure examinations have always been a challenge. The threat of cheating and unauthorized access by miscreants has always remained up. Even the manual supervision has failed to stop such unauthorized access perfectly. Quality students are main hope for the better economy and better future. Examination environment includes the entire staff associated with it, infrastructure, computers, rooms, and buildings, boundary walls, supervising staff and the network connectivity and integrity Filtering through quality assessment and secure examination will yield the quality students. This paper gives some of the simple and economic methods to avoid the unauthorized access in the online examinations:

a) Secure Personal Identity (SPI) using fingerprint recognition and biometrics:

To identify every student in a huge crowd of 500 students is difficult in manual examinations. It may require many checking personnel and long hours. This problem could be easily solved in the online mode of examination. Faces can match but the fingerprints will be different. The use of fingerprint recognition and matching technique will strictly identify the fingerprint patterns. In addition to this the biometric devices will keep track of the arrival timings of the students. For a crowd of 500 students we have deployed 20 biometric devices that will be used to manage a group of 25 students each. The use of biometric identification has also lead to increase in efficiency. Instead of serving a long queue for checking the students' I.D before letting them inside an examination room, the biometrics helps schools to avoid backed-up, unauthorized entry, fake I.D. cards. In a survey it was found that a school system where biometric devices where used instead of PIN pads. With a number of students standing outside examination halls each and every minute saved can prove precious in not

only helping students accommodating themselves better before an exam when inside the room but also helped the school authorities in curbing any mal practices.

b) Security Based on Enrollment and Client IP:

Every student will have his own machine assigned with a unique static IP address. This IP will no more be accessed by another student throughout the ongoing examination session. The virtual machine keeps track of the ongoing examination on particular IP clients. If the server has static IP address xxx.xxx.xx.100, the next 500 clients will have the IP in ascending sequence from xxx.xxx.xx.101 to 500. After assigning the static IP address to all clients manually, it is important to check the connectivity of every client with the server respectively. The address of server is pinged from every client node one by one. Every client has a visible enrollment number plate. Every 10 candidates are regularly being monitored by sensor nodes. The special exam group is created by grouping the hostnames / IP of clients for a specific location (Computer Lab) and time. To avoid the malpractice in the exams we use different types of biometrics as a means to log into the exam. We use the camera and finger print scanner to identify the students. The user after identified login into the system uses the user-id and password provided by the supervisor, which are authenticated by the server. This gives them permission to logon to the examination web page otherwise the students cannot login into the system. The unauthorized users attempting to log into the system from remote computers are blocked by the proposed system. Once the session begins the timer is on, the student completes his exam within the allocated time and once the time is up the system send an alert and logs the user off. The answer scripts will be fetched by server as per the corresponding sequence of IP & enrollment numbers. The application of IP addressing purely on a topographic basis does not create an environment in which concise security policies are easily created. This fact, in conjunction with the IP address dependencies of many security features, can lead to overly complex device configurations. The assignment of IP addressing using a role-based methodology is the most effective way to reduce this complexity. This methodology will allow for the simplification of many network device configurations as well as the creation of succinct ACLs that will be easier to add and maintain. With a role-based addressing methodology, interface IP addresses are assigned from pools dedicated to specific device roles. After administrators employ a role-based address assignment, there will be new avenues through which they can implement additional security controls. For example, if administrators are sure that all addresses in the subnet xxx.xx.xx.101/125 represent loopback interfaces of core network devices, they can safely leverage that information throughout the network.

c) Securing the Entire Examination Environment using Sensor Nodes (SESEN):

The SESEN is a broader term introduced here to show to use of sensor nodes in securing the entire examination environment. It includes all the personnel, infrastructure, client machines, rooms, buildings, surroundings and the server room itself. The WSN Technology (Wireless Sensor Networks) is composed of unique devices known as nodes that have ability to sense the environment and communicate the sensed information gathered from the monitored field to the base through wireless networks. The sensed information is routed to the base through multiple hops. In our proposed model we have taken 50 sensor nodes for deployment in the multi campus environment besides having 20 nodes at standby for any possible replacement or vice versa (Fig. 1). These all nodes will communicate to the base. The base station can use it locally or is broadcasted to other networks including internet through gateways. The sensor nodes can be mobile or immobile. However the security breaches in WSN networks active in any particular area might lead to worst consequences often, so it is important to protect

wireless sensor networks and its sensitive devices against such threats. Attack on WSN communication channels and hardware devices have always been a serious matter of concern. To have a secure communication throughout, a sophisticated cryptographic mechanism can be employed to protect the WSN communication from various possible attacks [2]. Snooping on captured WSN data can be tackled by various encryption methods, and the inoculation of unfavorable messages by the attacker can be prevented by the authentication processes.

However, a direct physical access to the nodes allows an attacker to manipulate the nodes at random. In particular, sensor nodes could be compromised or programmed to execute malicious code inoculated by the attacker. Tamper Resistance Mechanisms (TRM) applied to

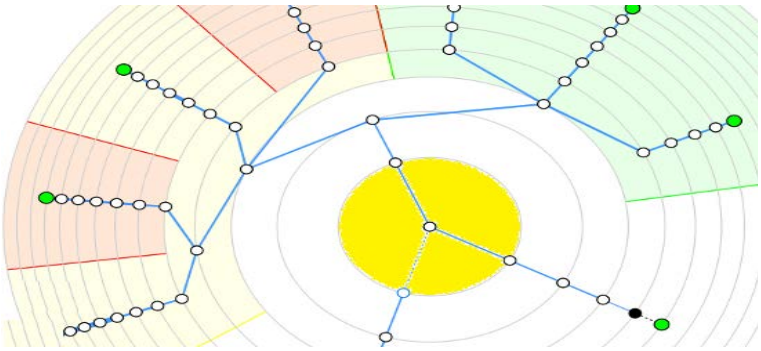

Fig. 1: A 50 Node Sensor Network Deployment in 5 Buildings

the nodes, hardware, concealment, surveillance and other techniques may be used to mitigate such attacks. However, they cannot be completely prevented and therefore, any communication security scheme being used must be sufficiently resilient to tolerate a certain amount of compromised nodes. Consequently an important objective is to limit the impact of a set of compromised nodes on the legitimate operation of the network to a minimum. This objective can optimally achieved by authenticating mechanisms that establish security relationship between communicating end-points [3]. This limits the influence that a single compromised node has to its own resources. Thereby, it cannot tamper with messages that originate at other nodes. With the secret key agreement in sensor networks based on locally shared keys, a multi hop communication can be employed and protected using an interleaved message authentication scheme. Sensor nodes and their memory requirements can be adapted to the required security level and the available resources. Based on keys shared between nodes within a neighborhood, a message authentication scheme can be thus devised that will allow secure transmission of messages even over long distances with real-time monitoring and sensing [4]. The proposed security mechanism protects the integrity of messages that are exchanged within networked sensors or to the base for onward exchange via internet. The attainable level of security is that an attacker is given a moderate level of strength that is able to capture a fraction of all nodes, comparable to that provided by end-to-end security mechanisms at a significantly lower cost in terms of computational resources. The focus of monitoring missions is to acquire and verify information about potential threats and positions of sensitive environmental locations. Once the event has been detected, the nodes will collect information and then use one of many different types of algorithms to calculate the current location of the object relative to the node locations [5]. From here it is the goal of the sensor network to track the object or its associated events as it moves through the sensor network.

III. Resource Topology, Framework and Project Implementation:

Computer network topology is the way various components of a network (like nodes, links, peripherals, etc) are arranged. Network topologies define the layout, virtual shape or structure of network, not only physically but also logically. The way in which different systems and nodes are connected and communicate with each other is determined by topology of the network. Topology can be physical or logical. Physical Topology is the physical layout of nodes, workstations and cables in the network; while logical topology is the way information flows between different components [6]. The volume of data that can be transferred across a network at a given time is called its bandwidth. An expensive, high bandwidth network is able to transfer data much quicker than a low bandwidth one. The bandwidth is affected by the types of network cards and modems used as well as the amount and type of cable used. Also, the way in which computers are connected together to form a network has a large effect on its speed and efficiency. There are a number of different ways to connect computers in a network - but these are the most common:

a) Network Topology used in the Environment:

There are many topologies that can be used in any model. We gave preference to a mixed kind of topology that will use the features from bus and star topologies i.e. tree topology. A tree topology is essentially a combination of bus topology and star topology. The nodes of bus topology are replaced with standalone star topology networks. It has a root node, intermediate nodes, and ultimate nodes. This structure is arranged in a hierarchical form and any intermediate node can have any number of the child nodes. In this topology, the computing device can have maximum one or two connections, so we cannot attach more than 2 child nodes to the computing device (or parent node) [7]. There are many sub structures under tree topology, but the most convenient is B-tree topology whereby finding errors is relatively easy. All the 500 clients will be interconnected and controlled by a server machine (Fig. 2). These clients are arranged in linear and star topological way or also called a tree topology. This topology can be chosen as per the building layout and the network requirements. We chose this topology because we are conducting examination of 500 students at a time in 5 different buildings of different layouts. It is based upon the physical hierarchical topology must have at least three levels in the hierarchy of the tree, since a network with a central 'root' node and only one hierarchical level below it would exhibit the physical topology of a star.

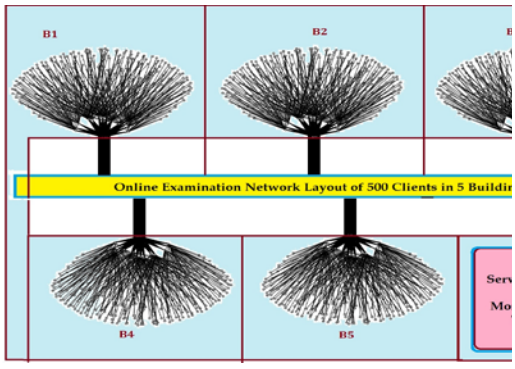

Fig. 2: Network Layout with 500 Nodes

It has physical hierarchical topology and with a branching factor of 1 would be classified as a physical linear topology [8]. The branching factor is independent of the total number of nodes in the network and, therefore, if the nodes in the network require ports for connection to other nodes the total number of ports per node may be kept low even though the total number of

nodes is large; – this makes the effect of the cost of adding ports to each node totally dependent upon the branching factor and may therefore be kept as low as required without any effect upon the total number of nodes that are possible. The total number of point-to-point links in a network that is based upon the physical hierarchical topology will be one less than the total number of nodes in the network. If the nodes in a network that is based upon the physical hierarchical topology are required to perform any processing upon the data that is transmitted between nodes in the network, the nodes that are at higher levels in the hierarchy will be required to perform more processing operations on behalf of other nodes than the nodes that are lower in the hierarchy. Such a type of network topology is very useful and highly recommended.

b) Implementation of the Project within Separate Buildings Interconnected:

The demo examination of this proposed work was conducted in the university campus with exact no. of clients and sensor nodes deployed accordingly in 10 different rooms of 5 different buildings with total no. of students for demo session as 300. All the client machines were mapped as per the project and connected to virtual machine on a dedicated server. All the 50 sensor nodes were connected properly and relayed transmission of the entire examination session to the base i.e. supervision team in the server control room. Examination started at 11:30 am to 12:30 pm. However students were asked to sit 15 minutes prior to the examination start time. The entire system worked very smoothly. Entries to all the examination blocks were continuously monitored and only the genuine students were allowed to sit in the examination. We had sent six fake students in a stealthy manner in crowd who were instructed to sit in examination. It was really an amazing experience because five were detected at the entry points and one succeeded to enter and managed to sit on a node. However he choose available the vacant seats and behaved like a normal student. It was only four minutes before the examination could start he was intercepted by monitoring cell in the server room with the help of smart sensor network in the examination area. The examination started sharp at the scheduled time and all the client machines were working fine. There was a dedicated power bank that didn't interrupt even for a second. Mostly all the students finished their exam in time and some remaining students were some were forced by the server and their session was finished by server itself as the time was up. At the end, server fetched all the answer scripts from client nodes and prepared the result. At 12:40 pm, server relayed a message on all the client nodes "Know Your Result! Click Here". After clicking the button, students were asked to enter their enrollment numbers to access their result/ marks obtained. They were shocked to see not their results, but the log of their moments and activities during the examination. For example the conclusive screenshot of the student no. 34 screen looks like Fig. 3. Server also flashed a colorful greeting message on client nodes i.e. "Thanks for being with us dear <Student Name>, wish you a very bright future ahead." At the bottom of screen there was a suggestion box that could be used by students to suggest something better to make this online examination system more secure and smooth.

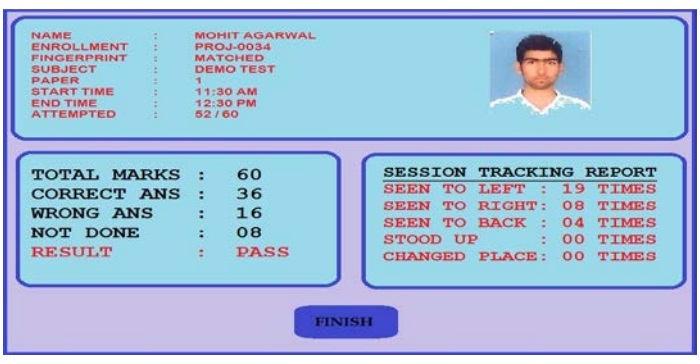

Fig. 3: Screenshot of Examination Window

IV. Conclusion:

The online examination is the only perfect mode of examination. It decreases the human interference and increases the standard. We realized the students were very happy with the online examination method especially using the biometric system and sensor network. Sensor nodes have the ability to sense the environment and to self organize automatically once programmed to do so. The Examination concluded with a smile and joy on everybody's face All the 50 sensor nodes were connected properly and relayed transmission of the entire examination session to the base i.e. supervision team in the server control room. Examination started at 11:30 am to 12:30 pm. However students were asked to sit 15 minutes prior to the examination start time. The entire system worked very smoothly. Entries to all the examination blocks were continuously monitored and only the genuine students were allowed to sit in the examination. This system of examination increases accuracy, perfection, examination culture and everything goes on smoothly without any human or robotic interference.

References:

[1] Arulogun, O. T. et al. (2014). Design and Development of a Security Surveillance System based on Wireless Sensor Network. International J Innovative Sc. Engg & Tech. Vol-1 (4), 07-09.

[2] F. Ahmad, Z. Eswawan (2005) "Wireless sensor network based system for fire endangered Areas", ICITA, 2 203-207.

[3] Gangi Raghu Ram et al. (2012). Tracking Objects Using RFID & Wireless Sensor Networks. International J Engineering Science & Adv. Tech. Vol-2 (3), 513 – 517.

[4] Gian Luca Foresti et al. (2009). Visual Sensor Technology for Advanced Surveillance Systems: Historical View, Technological Aspects and Research Activities in Italy, Sensors 2009, 9, 2252-2270.

[5] U. Hong Nhung Thi Nguyen (2005). Intrusion Detection in Wireless Sensor Networks. Ph.D. Thesis, University of Florida. 112 pp.

[6] T. J. Miling et al. (2009), Data Security and Transmission in Wireless Sensor Networks. Ph.D. Thesis, Tokyo University, Tokyo.

[7] K. Pits et al. (2011), Data Security on Wireless Sensor Network", IOP J. Phys., Conf. Series 52 12433-1-4.

[8] J. Q. Adams and A. A. Armstrong, "A Web-based testing: A study in insecurity," World Wide Web, vol. 1, no. 4, pp. 193–208, 1998.