The User Authentication and Key Arrangement Techniques using Advanced Encryption standard in Wireless Sensor Network

Jasmine Kaur[1], Sukwinder Sharma[2]
M.Tech (student), Assistant Professor
Department of Computer Science, Department of Information Technology
Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib

Abstract— Presently, wireless sensor systems are a novel technology industry with various applications. The nodes deployed in such a situation are uninhibited by anyone. Therefore, any security flaws can threaten future applications. Consequently, user authentication is an imperative problem for wireless sensor networks because it allows only authorized users to access real-time data from the radar nodes or cluster heads via a base station. In addition, due to the cost-constrained influence of nodes, presentation also is a crucial issue that must be considered. The concept of Internet of Things which is previously at our front doors is that each object in the Internet infrastructure is interconnected into a global active expanding network. Sensors and canny objects are beside classical computing devices key parties of the IOT. We can already adventure the assistances of the IOT by using various wearable's or smart phones which are full of diverse sensors and actuators and are associated to the II via GPRS or Wi-Fi. Since sensors are a key part of IOT, thus are wireless sensor networks. Researchers are already working on new techniques and efficient approaches on how to integrate WSN improved into the IOT situation. One characteristic of it is the security aspect of the integration. Recently, Turkanović et al., proposed an exceedingly effectual and novel user verification and key agreement scheme for heterogeneous WSN which was changed to the IOT notion. In this research we are Authenticated the user via Key Server which is running in Wireless sensor network. For user authentication under heterogeneous wireless sensor network the user joins to connect any wireless sensor node. It will redirect to Key server which is control all domains. The key server first check the undisclosed key which receive from user if it exists in their database then it sends one key based on Advanced Encryption Standard Algorithm (AES algorithm) and send to user so that whatever user enter the user name and password it gets encrypted first and then forward to key server. The key server receives the cipher message and decrypt the message and check user name and password if get match then user authentication get true in wireless sensor network. In this thesis, we proposition a secure and insubstantial authentication scheme for heterogeneous wireless sensor systems using smart cards. In addition, we use dynamic characteristics to prevent intimidations to users' privacy. Examines of the safety and presentation of our scheme demonstrated that it can achieve shared authentication and key arrangement among users, a base station, and collection heads; fight most possible attacks; and provide higher effectiveness than previous parameters.

Keywords— *User Authentication, Security issues, Wireless Sensor Network and AES encryption Techniques.*

I. INTRODUCTION

With the rapid development of the Internet and communication technology, wireless communication, such as wireless sensor networks and wireless ad hoc networks, has become an important part of our lives. Currently, there are two common topologies in a wireless sensor network, i.e., homogeneous and heterogeneous wireless sensor networks.

A wireless sensor network is consisting of spatially dispersed independent devices using sensors to monitor physical or environmental conditions. A WSN system includes a gateway that offers wireless connectivity back to the wired world and distributed nodes. Wireless Sensor Network is crucial for the future of Internet of Things since they cover a wide application range essential for the IOT [1]. They are a system of small, wireless, ad-hoc sensor nodes also called motes, which are interconnected and positioned in an area of interest (e.g. home, forest, battle field, etc.). They are used in a wide range of application situations, like military, healthcare, environment, home, etc. The sensors nodes are resource constrained and thus have a limited dispensation power, transmission range and battery life. Since WSNs are evermore attached to the IOT singularity, they contemporary new challenges and opportunities. Wireless sensor networks (WSNs) are rapidly growing in popularity due to the low cost explanations for a variety of challenges in the real-world. WSN has no infrastructure support, is quickly deployed in a section with several low-cost sensor nodes, is employed for monitoring the environment, and is rigid to maintain its security. Multichip communication is preferred in WSN as the number of nodes is very large, and sensor nodes have restrictions with respect to power, computation, communication, and storage. Security in WSN becomes crucial since the nodes after the deployment cannot be manually maintained and observed. This situation becomes a major issue in WSN due to its network of communication [1].

The authentication is provided to the data that can be sent or opened by any node in the network. Also, it is critical to prevent and gain the information from the unauthorized users. As new intimidations and attack models are proposed, several kinds of authentication mechanisms have been introduced in WSN security.

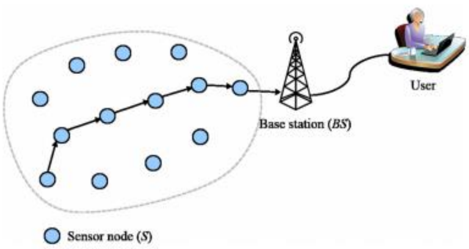

Fig.1 Architecture of a homogenous wireless sensor network [3]

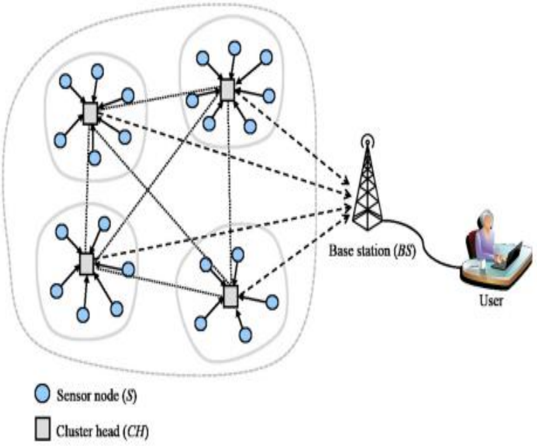

Fig.2 Architecture of a heterogeneous wireless sensor network

The most popular topology technology for decreasing the energy consumed by sensor nodes and increasing the lifetime of the network is the heterogeneous sensor network. Figure 2 shows that all of the sensor nodes of a heterogeneous sensor network can be divided into several clusters. Each cluster consists of a cluster head (a powerful sensor node) and a number of sensor nodes. The major differences between cluster heads and sensor nodes are their computational capabilities, storage capabilities, and transmission ranges.

The cluster heads possess greater battery power than the generic sensor nodes in order to perform more complicated operations, so they have better computational capability. Second, compared with generic sensor nodes, cluster heads have better storage capabilities due to their larger memory space. Third, cluster heads must have a larger transmission range than generic sensor nodes in order to ensure that the signal coverage reaches all sensor nodes within the cluster. The responsibilities of cluster heads are to collect, integrate, and[4] transmit the information gathered from their sensor nodes to the base station. Through the data integration and hierarchical transmission method, the architecture of a heterogeneous sensor network allows it to reduce the overall consumption of electrical power and reduce the workload, thereby extending the lifetime of the entire network.

Wireless sensor networks are subject to invasions and node capture attacks because they are deployed in public and unprotected locations. In addition, wireless communication is used between the sensor nodes and the base station, so it is easy for anyone to eavesdrop on the communications. Thus, it is necessary to consider the remote authentication issue, which allows only authorized users to access the information from the network.

A. *WSN Application*

Propels in wireless sensor networking and incorporation have empowered little, adaptable, minimal effort hubs that cooperate with their surroundings through sensors, actuators and correspondence. WSNs may comprise of various assorted sorts of sensor hubs to sense distinctive sorts of parameters that empower them to screen a wide assortment of encompassing conditions that incorporate the accompanying: flow, temperature, pressure, humidity, moisture, noise levels, mechanical stress, speed, etc. Savvy sensors that can screen numerous physical variables can be utilized with WSN.

- Habitat Monitoring
- Military Applications
- Physiological Monitoring
- Vehicle Tracking[5]

II. AUTHENTICATION

In Wireless Sensor Networks Authentication is a process by which the individuality of a node in a network is established and guarantee that the data or the control messages originate from an authenticated source. Authentication mechanism can be differentiated based on the [3] following criteria:

(i) Authenticate uni-cast, multicast, or broadcast messages

(ii) Shared key or asymmetric (public key) cryptographic method

(iii) Static, mobile, or both aspects of WSN.

A variety of researches have focused on point-to-point authentication mechanism, which validate uni-cast messages in WSN. In spite of being secure, uni-cast methods cannot be applied straight to either multicast or broadcast messages. Broadcast messages are straight obtained from the reliable sources and cannot be changed during transmission [4].

The basic components of a broadcast authentication process are:

(i) Examination the source identity from which the message originate,

(ii) Confirm the message truthfulness for ensuring the message originality.

Various authentication procedures consist of:-

(i) One-way authentication,
(ii) Two mode or mutual authentication,
(iii) Three mode authentication,
(iv) Contained authentication.

III. ADVANTAGES IN WSN

A. *Energy saving:* Mobile agent removes data fusion as well as processing from sensor node to agent; data are ready-made when agent is actually relocating [4]. This may lessen data targeted visitors from the network, help save network bandwidth, lessen end-to-end hold off as well as enhance support responsiveness. Thus mobile agent could possibly lessen energy consumption effectively, as well as increase network lifetime.

B. *Simplify network protocol:* WSN is actually a type of application-oriented network, which in turn demands the unique desire connected with various individual needs to be understood by simply network protocols, from application layer to network layer as well as data link layer. System protocols are situated throughout reduce tiers connected with nodes software program, so intricate protocols are difficult to development and gaze after, and they are an easy task to create network breakdowns. Mobile agent could possibly know users desire as well as encapsulate network protocols in the reduce layer. While user's desire is actually modified, solely the actual agent needs to be modified as well as network protocols stay the identical [6].

C. *Flexibility and autonomy:* This mobile agent may be reprogrammed; new agent may be injected into the network in any time as well as redistribute duties; furthermore, a single sensor node could possibly function a number of agents simultaneously. And then network mobility as well as versatility are much better. Moreover, mobile agent could possibly comprehend natural environment modify separately as well as create reply rapidly, as well as maintain the system with perfect condition.

IV. REQUIREMENT OF WIRELESS SENSOR NETWORK

Before going into the definite investigation of routing conventions, a brief depiction of the considerable number of variables that influence the working of these conventions are contemplated. Contingent on these variables, a few decisions about the conventions working are drawn. The execution of remote sensor systems depends on the accompanying components.

A. *Latency:* Latency is characterized by the amount of time a hub takes to sense, or screen and imparts the action. It likewise relies on upon the current application. Sensor hubs gather data, process it and send it to the destination. Latency in a system is figured taking into account these activities and in addition the amount of time a sensor takes to forward the information in substantial load traffic or in a low density system.

B. *Energy Awareness:* Every hub utilizes some vitality for activities like sensing, processing, storage and transmission. A node in the system ought to know the amount of vitality will be used to perform another errand that is presented, the measure of vitality that is dispersed can fluctuate from high, moderate to low depending on the kind of usefulness or movement it needs to perform.

C. *Scalability:* Scalability is an essential variable in remote sensor systems. A system region is not generally static, it changes relying on the user necessities. Every one of the hubs in the system zone must be versatile or ready to alter themselves to the adjustments in the system structure contingent on the user.

D. *Network Power Usage:* All the sensor nodes in the system utilize a sure measure of system force which helps them to perform certain activities like sensing or processing or even forming group's network power usage.

E. *Node Processing Time:* Refers to the time taken by the hub in the system for performing all the operation beginning from the detecting action to handling the information or putting away information inside of the supports and transmitting or getting it over the system [7].

V. RELATED WORK

Z. Cheng et. al. [2006] proposed an energy-efficient routing paradigm that used information conglomeration and in-system handling to boost the system lifetime. Because of the hub stationary and greatly low portability in numerous applications in WSNs, a sensible methodology is to orchestrate hubs in a settled topology. A sans gaps methodology was utilized to fabricate bunches that are altered, equivalent, neighbouring, and non-covering with symmetric shapes. Square groups were utilized to get a settled rectilinear virtual topology. Inside every zone, a hub was ideally chosen to go about as bunch head. Information accumulation was performed at two levels: nearby and after that worldwide. The arrangement of bunch heads, likewise called Local Aggregators (LAs), performed the neighbourhood collection, while a subset of these LAs was utilized to perform worldwide conglomeration. Be that as it may, the determination of an ideal choice of worldwide accumulation focuses, called Master Aggregators (MAs), is NP-difficult problem [8]. **Stanislava Soro et.al.** [2005] investigated diverse coverage-aware expense measurements for the bunch's determination head hubs, active nodes and routers in remote sensor organizes whose point is to keep up scope of an observed space [9]. In such scope saving applications, both the remaining vitality of the sensor hubs and also the excess in their scope must be mutually considered while deciding the best possibility for group head hubs, dynamic hubs and information switches. Through broad recreations, they delineated the inadequacies of utilizing remaining vitality or scope repetition as the main criteria for the choice about the hubs' parts in bunch based remote sensor networks [9]. **Stanislava Soro et. al.** [2005] investigated diverse coverage-aware expense measurements for the bunch's determination head hubs, active nodes and routers in remote sensor organizes whose point is to keep up scope of an observed space [10]. In such scope saving applications, both the remaining vitality of the sensor hubs and also the excess in their scope must be mutually considered while deciding the best possibility for group head hubs, dynamic hubs and information switches. Through broad recreations, they delineated the inadequacies of utilizing remaining vitality or scope repetition as the main criteria for the choice about the hubs' parts in bunch based remote sensor networks [9].

VI. PROBLEM FORMULATION

Security in wireless sensor networks becomes critical since the nodes after the deployment cannot be manually maintained and observed. This situation becomes a major problem in WSN due to its network of announcement. The authentication is provided to the data that can be sent or accessed by any node in the network. Also, it is critical to prevent and gain the information from the unauthorized users. As new threats and attack models are proposed, several kinds [11] of authentication mechanisms have been introduced.

VII. OBJECTIVES

- To study the concept of authentication concept in the wireless network system.
- To proposes a new and improved user authentication and key agreement scheme for heterogeneous WSN.
- To implement Advanced Encryption Standard Algorithm for the same purpose.
- Compare our results with previous work

VIII. SIMULATION MODEL

In this research we are Authenticated the user via Key Server which is running in Wireless sensor network. For user authentication under heterogeneous wireless sensor network the user joins to connect any wireless sensor node. It will redirect to Key server which is control all domains.

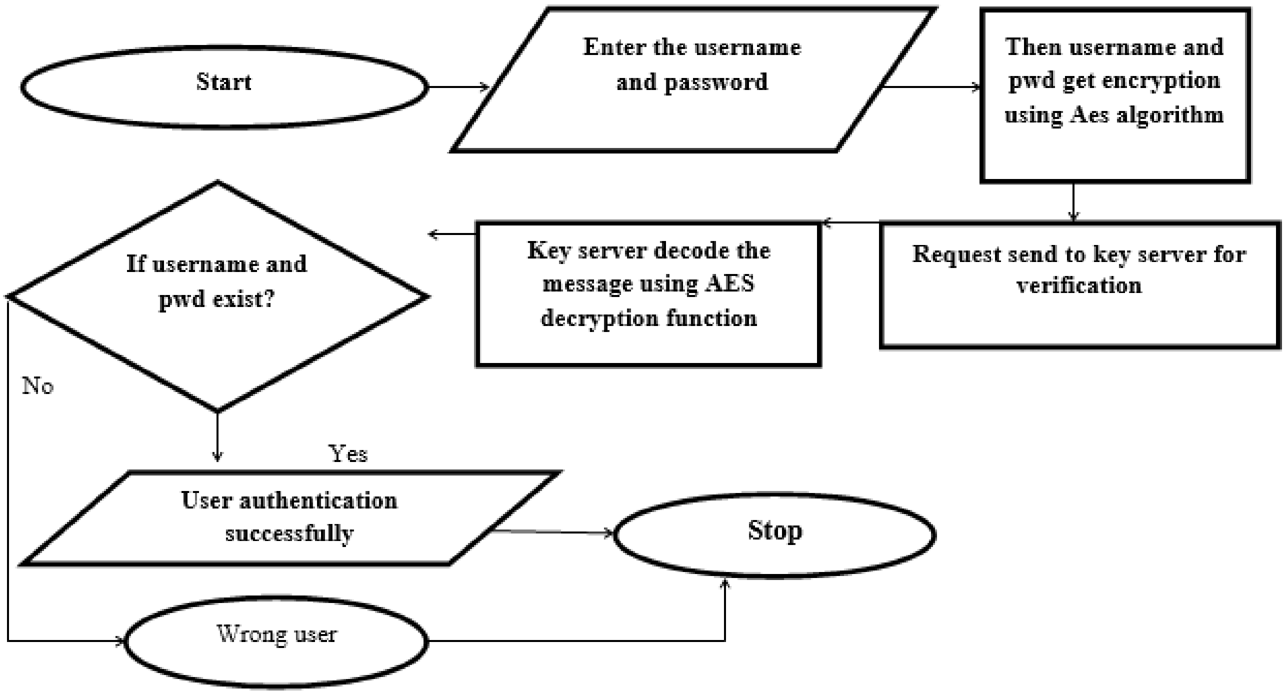
Start
Enter the username and password
Then username and pwd get encryption using Aes algorithm
Request send to key server for verification
Key server decode the message using AES decryption function
If username and pwd exist?
No
Yes
User authentication successfully
Stop
Wrong user

Fig.3: Proposed Work

The key server first check the secret key which receive from user if it exists in their database then it sends one key based on Advanced Encryption Standard Algorithm (AES algorithm) and send to user so that whatever user enter the user name and password it gets encrypted first and then forward to key server. The key servers receives the cipher message and decrypt the message and check user name and password if get match then user authentication get true in wireless sensor network.

IX. RESULT ANALYSIS

In this section, after the completion of implementation work, there is dire need to check the efficiency of user authentication based on AES with comparison to other techniques. In this section, we compare the results of proposed technique (AES) with existing technique. In the user authentication key agreement technique during the registration phase client has the secrete key. To overcome this drawback we use AES 128 bit technique for user authentication because in this technique key server send the secret key to client for completion of registration phase. In the existing technique the login phase include user name, password and secrete key to verify. But in the purposed technique the login phase include the name, password and secrete key encrypt with AES encryption to verify.

- **Registration Phase**

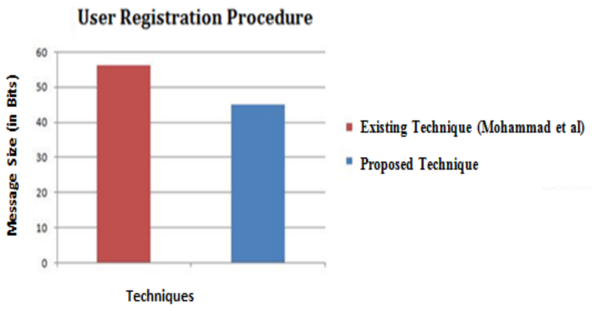

Fig.4 Registration phase graph

Above figure no: 4 describes the comparison of byte value which is used to complete the registration phase in existing and proposed technique. In this existing technique (Mohammad et al) indicates 56 byte which is computed with existing technique and research technique indicates 42 byte which is computed with the purposed technique (AES 128). Firstly complete the registration step after that create the password and login id in main server.

- **Receiving Response from Main Server**

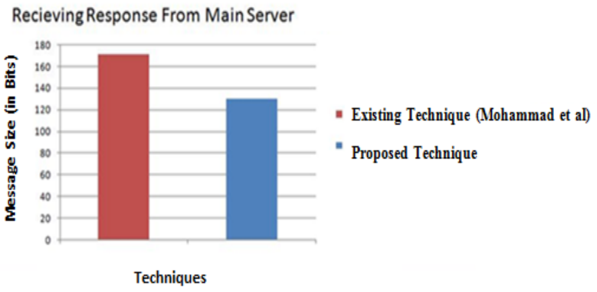

Fig.5 Receiving Response from Main Server Graph

Above figure no: 5 describes the comparison of receiving response from main server in existing work and proposed work technique. In this existing technique (Mohammad et al) indicates 171 byte which is computed with existing technique and research technique indicates 130 byte which is computed with the purposed technique (AES 128).First, sign in the page and then receiving the reply from main server.

- **Receive Authentication Message from Server**

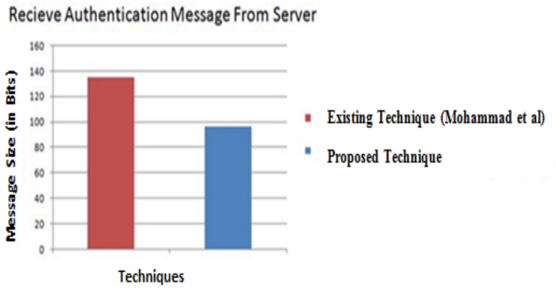

Fig.6 Receive Authentication Message From Server Graph

Above figure no: 6 describes the comparison of the byte value of receiving the authentication message from the server. It describes the bytes are used in existing and purposed technique to get the authentication message from the server. In this existing technique (Mohammad et al) indicates 135 byte which is computed with existing technique and research technique indicates 96 byte which is computed with the purposed technique (AES 128). In this, Login page create User name and password then user login id and get the authentication message from the server side.

- **Login Protocol Function of Number of Clients**

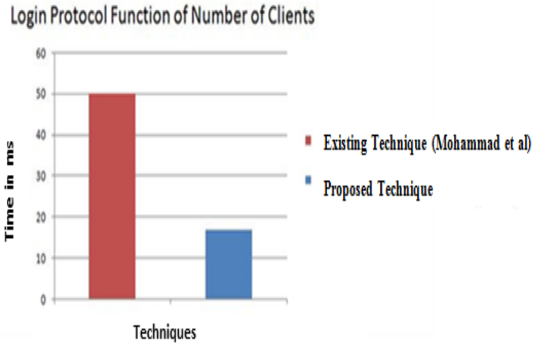

Fig.7: Login Protocol Function for Number of Clients Graph

Above figure no: 7 shows the comparison of login protocol function of number of clients in existing and proposed technique. In this existing technique (Mohammad et al) indicates 50 ms which is computed with existing technique and research technique indicates 17 ms which is computed with the purposed technique (AES 128). It computed the login time of clients, which are already registered on the server.

- **Computation after Receiving Authentication Message**

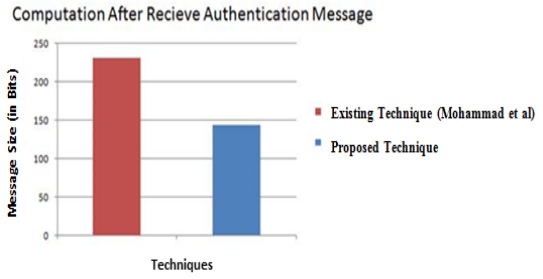

Fig.8 Computation after receiving authentication Message Graph

Above figure no: 8 describe the computation after receive authentication message .it describe the byte value which is used to performance computation. In this existing technique (Mohammad et al) indicates 230 byte which is computed with existing technique and research technique indicates 144 byte which is computed with the purposed technique (AES 128). Computation is done after receiving the authentication message the secure information.

X. DISCUSSION

This section describes the detail of experimental results of our user authentication encryption method with factors like registration phase, receiving response from main server, receive authentication message from server, login protocol function for number of clients and Computation after receive authentication according to proposed algorithm. It also provides us the comparison of our proposed idea with the existing technique of user authentication and key agreement scheme for heterogeneous wireless sensor network.

Table no: 1 Factors for Comparison

Factors	Existing Technique Results [10]	Proposed Technique results
Registration phase	56 bytes	42 bytes
Receive response from main server	171 bytes	130 bytes
Receive authentication message from server	135 bytes	96 bytes
Login protocol function for number of clients.	50ms	17ms
Computation after receiving authentication message	230 bytes	144 bytes

Above table 1, describes the comparison of factor computation of proposed technique. In this existing technique value or paper value is that value which is computed in existing technique and research value is that value which is computed with the help of proposed technique (AES 128).

XI. CONCLUSION

In this paper, we proposed a more secure, efficient, and active user authentication scheme using smart cards for assorted wireless sensor networks. Safety analyses showed that our proposed scheme can prevent well-known attacks and indeed achieve mutual authentication and session key agreement. Our apply the Encryption technique It is a web instrument to clamber and decode content exploiting. AES encryption calculation. You can choose 128, 192 or 256-bit long key size for encryption and unravelling. The consequence of the procedure is downloadable in a content record. AES is a symmetric encryption calculation. Our detailed comparisons of our scheme and related schemes showed that our scheme provided better performance. As a result, our proposed scheme is more suitable for application in wireless sensor networks.

XII. REFERENCES

[1] Chang, Chin-Chen, Wei-Yuan Hsueh, and Ting-Fang Cheng. "A Dynamic User Authentication and Key Agreement Scheme for Heterogeneous Wireless Sensor Networks." *Wireless Personal Communications*: 1-19.

[2] Turkanović, Muhamed, BoštjanBrumen, and Marko Hölbl. "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion." *Ad Hoc Networks* 20 (2014): 96-112.

[3] Yang, Jen-Ho, and Chin-Chen Chang. "An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem." *Computers & security* 28, no. 3 (2009): 138-143.

[4] Wen, Fengtong, and Xuelei Li. "An improved dynamic ID-based remote user authentication with key agreement scheme." *Computers & Electrical Engineering* 38, no. 2 (2012): 381-387.

[5] Juang, Wen-Shenq. "Efficient multi-server password authenticated key agreement using smart cards." *IEEE Transactions on Consumer Electronics*50, no. 1 (2004): 251-255.

[6] Liao, Yi-Pin, and Shuenn-Shyang Wang. "A secure dynamic ID based remote user authentication scheme for multi-server environment." *Computer Standards & Interfaces* 31, no. 1 (2009): 24-29.

[7] Z. Zhang, Y. He, Y. Ji, X.S. Shen, "A new energy efficient approach by separating data collection and data report in wireless sensor networks", Proceedings of the International Conference on Communications and Mobile Computing, 2006.

[8] M. Golsorkhtabar, F. K. Nia, M. Hosseinzadeh, Y. Vejdanparast, "The Novel Energy Adaptive Protocol for heterogeneous wireless sensor networks", Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on (Volume:2), 9-11 July 2010, Page no. 178 – 182, DOI: 10.1109/ICCSIT.2010.5563781

[10] StanislavaSoro, Wendi B Heinzelman, "Prolonging the lifetime of wireless sensor networks via unequal clustering", Parallel and Distributed Processing Symposium, 2005. Proceedings.19th IEEE International, 2005, 8 pp.

[11] M. Qin, R. Zimmermann: VCA, "An energy- efficient voting-based clustering algorithm for sensor networks", Journal of Universal Computer Science 13(1), 2007.