A Context-Based User Authentication Scheme for Ubiquitous Services

Samyama Gunjal G H, Pallapa Venkataram, and G Narendra Kumar

***Abstract*—With the development of Internet and network technology, Ubiquitous computing is widely enabled. Ubiquitous environment is confronted with many unique challenges. Authentication, Authorization and Accounting (AAA) is one of the most challenging security problems in ubiquitous environment due to its feature of providing anytime anywhere services. Existing authentication schemes aim at only entry-point authentication, which may not suite the dynamic Ubiquitous environment. We propose an authentication scheme which is based on user context information. Whenever a user moves into Ubiquitous service environment, system at first, collects the context and provides the best unique User Certificate to access the preliminary services. For quick and fast context evaluation, we apply genetic algorithm for the context selection, trust evaluation and credential verification of authenticated user. The designed authentication has been tested in a ubiquitous museum environment. The results are quite encouraging.**

***Index Terms*—Ubiquitous Computing, Evolutionary algorithm (EA), User AAA.**

I. Introduction

WITH the development of the Internet technology, the Ubiquitous computing is widely enabled. Anywhere, any-time services are provided to all the affiliated users in ubiquitous environment. There is a free flow of information between the Ubiquitous services (UbiSS) and the ubiquitous user [1] [2]. Attention has to be paid on the information security since it is prone to security problems by the network distributed features. A strong authentication scheme is needed to establish the trust between the UbiSS and the user. The traditional authentication methods include passwords, digital certificates, biometrics, etc., which have their own advantages and ambiguities [3].

X.509 digital certificates are currently widely used, which are PKI based certificates, whose absences means that the content sent or received, can potentially be seen by other parties and vulnerable to security threats. PKI system confirms the integrity of the certificate, and provides scalability and non-repudiation services.

a) Ubiquitous Scenarios: User identification, authentication and authorization is an essential and pre-requite process in ubiquitous environment, to avail the services of UbiSS. This can be done with user certification [4] [5]. Current existing certification process are static, which are not suitable for ubiquitous environment. Consider the following scenarios:

- *Scenario 1*: A user is currently using Museum UbiSS, where he/she is presented with artifacts/exhibits information. As he moves from one exhibit to another, context changes and exhibits information also keeps changing. After some time, user may wish to visit nearby shopping mall. This triggers Shopping UbiSS, which has to adapt to new environment, and continue to provide the relevent services.
- *Scenario 2*: A user is currently using Health-care UbiSS, comprising of a *hospital* and a *medical college*. Consider a post-graduate intern, who will be a student at the college and a doctor at the hospital treating patients. UbiSS needs to adapt to the changing patient environment and continue the services.
- *Scenario 3*: A user is currently using Home UbiSS, where he/she is using a Smart Phone. After some time, user may wish to use his tablet. UbiSS needs device adaptation and allows the user to continue with the services using new chosen device.

Considering the scenarios, there is a need to identify the same user in different situations[6]. Now the query is *Does user certificate needs to change for the same user:*

1) ***using different Ubiquitous application services***?
2) ***using different Ubiquitous Devices***?

As same user has to be identified in different situations, Authentication scheme should be *user-centric* and should be based on *context* of the user. We present an user authentication scheme as an approach to adaptive user identity certificate based on user context using genetic algorithm (GA).

b) Proposed Work: In this paper, we propose context based certificate for users AAA purpose in ubiquitous environment. We exploit the *Evolutionary algorithm: Genetic Algorithm* to analyze the retrieved context for the adaptive dynamic scenarios, and generate user certificates. The Proposed scheme uses limited computational and storage resources, so that they are suitable for ubi devices. Overview of User Authentication Scheme is given in Fig.1.

The current work focuses only on the first scenario. Authentication on ubiquitous device adaptability is future work.

c) Organization of rest of the paper: The rest of the paper is organized as follows: section 2 gives information about some of the related works, section 3 gives the details of proposed authentication scheme, section 4 illustrates the simulation and results, and section 5 concludes the work.

Samyama Gunjal G H, Research Scholar, Protocol Engineering and Technology Unit, Electrical Communication Engineering Department, Indian Institute of Science, Bangalore, India, (Ph: +91-80-22932282), (email: s_gunjal@ece.iisc.ernet.in).

Pallapa Venkataram, Professor, Protocol Engineering and Technology Unit, Electrical Communication Engineering Department, Indian Institute of Science, Bangalore, India, (Ph: +91-80-22932282), (email: pallapa@ece.iisc.ernet.in).

G Narendra Kumar, Professor, Department of Electronics and Communication Engineering, University Visveswaraya College of Engineering, Bangalore, India, (email: gnarenk@yahoo.com).

ISBN: 978-988-19252-0-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

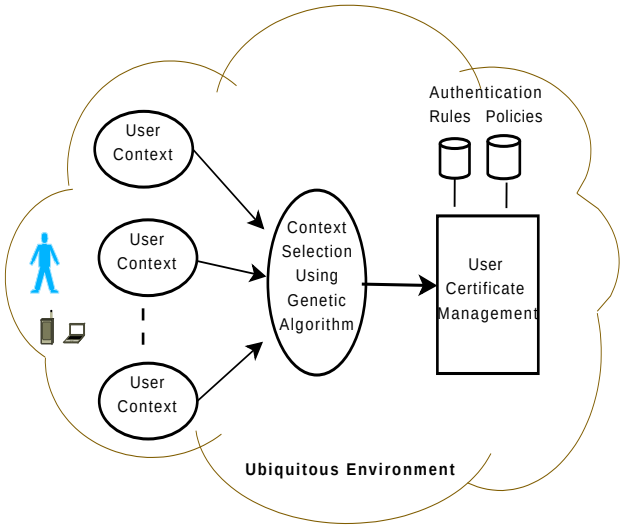

Fig. 1. An Overview of User Authentication Scheme

II. Related Works

Existing works on ubiquitous computing focus on issues like: finding communication designs, better QoS, routing, etc. User and device authentication issues are dealt with static convention schemes. Following are some works in ubiquitous environment.

OpenID [7] is a decentralized network authentication protocol. It overides the dependency on central systems for user identification. User create his account and use them for signing onto websites.

Host Identity Protocol(HIP) [8], discusses about implementing ubiquitous network securely. They consider the authentication cost of the network admin with DNS operator, who can verify the packets and do traceability test, and detect the eavesdropping and ensure the non-repudiation of packet also.

The work in [9] presents a authentication based on senors. Its a physical possession of moblie device for authentication. On shaking the device near the public terminal, device inturn, user is authenticated. User gestures and realted symbols are generated and authenticated.

In [10], an authentication scheme is proposed where admin facilitates the user and their objects service identification. On access to the resources by the user, the system checks the credentiality stored in the repositories and authenticates the user to use them.

Amigo [11] refers to the secured authentication between devices in its proximity by secure pairing. Using the knowledge of device 's physical nearness, co-located devices are mutually authenticated and verified. It overides the user involvement in verification and validation of the authentication process.

UC-TBAS [12] is a cognitive agents approach for intelligent and dynamic authentication scheme. The scheme automatically authenticates the user with less intrusion. It uses various metrics like transaction sensitivity, context sensitivity, and beliefs on user behaviors generated by ubiquitous commerce.

In [13] Identity-based signatures are used for authentication and role-based access control. Users role is decided which forms the identity of the user and leads to identity based authentication. Keys with respect to the roles are generated and assigned to the user for further usage.

III. Proposed Work

The UbiSS provides the user with functionalites of registration, authentication and authorization to avail ubiquitous services. In this section we present the fundamental concepts of our proposed context-based user authentication system: *With the changing user context, how user identity has to be managed and be adapted to the current situation, What privileges need to be provided to the user to utilise the services in the changed context*

UbiSS validates a user identity on registration and generates a certificate for that user and signs the certificate [13] [14]. It fills essential fields when generating a new certificate, including unique number as user ID, user name, issuer, subject, etc. The certificate validity is an important field in our scheme. Here the UC validity is either context dependent or time-dependent, whichever is earlier. Other fields that must be included in certificate are context based.

We have adapted the Genetic Algorithm and the weighted scheme for prioritizing the context, aiming for the better selection of the context. We generate the User Certificate (UC) once, and it keeps evolving as the context changes. Based on UC, user is provided with required service access.

Assumption: User current context are available instantaneously and are fine-grinded to use.

A. User Certificate(UC) Generation

A user in ubiquitous environment is ensembled with many context elements which fall roughly into different categories like: personal related, message related, time related, history related, activity related, physical environment related, etc. All categories are managed by context handler as:

- **User trivial information/context** - are user shared mandatory information and are not subjected to frequent changes,(as in: UserID, name, DOB, Sex, qualification, profession, etc.)
- **Retrieved context** - obtained at that particular situation(Physical context, Environment context,etc.)
- **History context** - the previous logs of user actions which are available in the history databases.

User certification techniques deploy the usage of hashing algorithms to compute the hash digest/fingerprint of data and this data is signed by the UbiSS private key [15] [16].

User uses this certificate to prove their legitimacy and avail the services.

Choosing user data for fingerprinting(FP) is an important phase in the proposed authentication scheme. We choose user data based on context, generate two FP's: FP1 and FP2, sign FP's: S1 and S2 and generate UC.

- User context are gathered and segregated accordingly.
- Fingerprint FP1 is computed with user trivial data by hash function SHA1.
- Public and Private Key pair are retrieved by PKI.
- FP1 is encrypted to Digital signature S1 with Private Key.
- Fingerprint FP1 is computed with user's selected context by hash function SHA1.

ISBN: 978-988-19252-0-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

- FP2 is encrypted to Digital signature S2 with Private Key.
- FP1, S1, FP2, S2, Public Key are combined to form UC.
- $FP1, S1$ used for user identification.
- $FP2, S2$ used for user access profile identification and authorization.
- Signed UC are stored on both UbiSS side and user side.

User Certificate Generation Protocol is given in Fig.2.

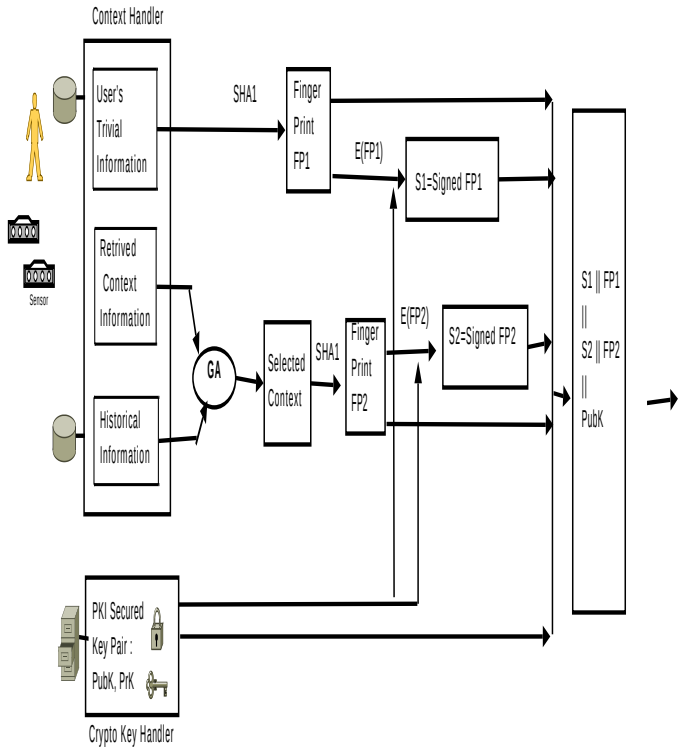

Fig. 2. Architecture of the User Certificate(UC) Generation Protocol

Now the query is which context are need to be chosen for creation of FP's, so that context-based FP's are generated, to mimic the user profile. We employ the Genetic Algorithm for this purpose [17].

B. Genetic Algorithm

Genetic algorithms (GA) are the popular searching strategies guided by the principle of Darwinian evolution [17]. It is an evolutionary algorithm based on selection, crossover and mutation functionalites on a population of chromosomes. The goodness of each chromosome is evaluated by the fitness function. If the chromosome has better and good fitness, the chance of its selection for the reproduction process is higher, as it survival chance is more. The evolution procedure is repeated until a user-specified termination criterion is satisfied.

C. Context Selection using GA

As stated earlier, ubiquitous environment has many types of context. Selection of Context that are informative is critical task. The context deemed to be the most effective need to be retrieved. Not all context are relevent, but distinguishing the relevant and irrelevant context is a tedious process. The problem we want to solve is finding the optimal context information based on the current situation and the users requirement that satisfies to certify the user.

Genetic algorithms are the support tool which permit all possible context information to be considered for inclusion in the user identity. Initial set of context types are created a prior by UbiSS, which forms the search space. The time required for the exhaustive context search increases as the search space grows. Hence we opt the heuristic search method for the fast finding of context information's.

Heuristic goal: To find optimal context information based on the user current situation and requirements.

1) Context as genes: We model context information as a chromosome where each individual context is a gene. In our approach, the chromosome do not have fixed number of genes. The issue in genetic algorithm is, encoding the set of chromosomes. We encode context information into chromosomes because our goal is to find optimal context information from the pool of Context in ubiquitous environment, which will be used in UC.

Individual Context - Genes
Collection of Context - Chromosome
Pool of context - Population
Weight of context - Fitness of Chromosome

A context $C(t)$ is the current context of the user and his environment at time t. It is a collection of n context that are used to represent that particular situation of the user at that time and is defined as $C_i(t) = \{c_1(t), c_2(t), ..., c_n(t)\}$

A context priority $cP(t)$ represents the priority assigned to context $C_i(t)$.

2) Fitness Assignment - Prioritizing Context: In each cycle/iteration of the genetic algorithm, each chromosome, in turn *gene*, must be evaluated.

We consider a weighted approach for assignment of priorities in our scheme.

- Let cp be the number of context priorities allowed and let $cP = \{1/cp, 2/cp, ..., n/cp, 1\}, (n < cp)$ be the available context priority. Weights are assigned for all prioritized context and these weights are used to for context selection and stored to historical databases.
- Let $w_t(C_i)$ be the priority weight of context C_i at time t. The GA initially searches the historical data for any prior existence of the context and if available, assigns that weight to $w_t(C_i(t))$.
- If the historical data is unavailable, the GA sets a default weight of $w_0(C_i(0)) = 1/cp$ to the context, where $w_0(C_i)$ is the initial priority weight of the context C_i.
- If weights have been specified for context elements in the rules and polices set, the corresponding weight is set as the initial weight for $C_i(t)$. Weight of context keeps changing over time.
- The weighted priority context $w_t(C_j(t))$ is calculated using Shannon's entropy [18]:

$$w_t(C_j(t)) = -\sum_{i=1}^{k} w_t(c_i(t)) \log w_t(c_i(t))$$

where $C_j(t) = \{c_1(t), c_2(t), ..., c_k(t)\}$

3) Context Selection: Context fitness of $C(t)$ are calculated and the chromosomes with maximun weight $w_t(C_j(t))$ is selected, where $C_j(t) = \{c_1(t), c_2(t), ..., c_j(t)\}$

ISBN: 978-988-19252-0-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

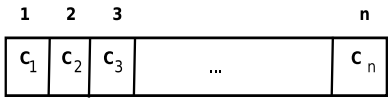

Fig. 3. Chromosome representation for n-context types

4) Context Crossover and Mutation: The original pool of context must remain up-to-date at all times. All (both historical and emerging) context must be re-evaluated each and every time a change has occurred. If the context are sorted by their priority values, a re-ordering is required. This make sure that the fitness values and the priority of the context are always up-to-date.

- UbiSS need to consider the changed context. Change means, either modification(upgrading/degrading) of current priority context or a emerging of new context. In both the cases, current context consideration is reviewed, and if required, is consider for the UC generation. New retrieved context are weighted accordingly and used, which form the new set of population to be searched.
- Crossover and mutation are the genetic operator used to produce new generations, i.e new offspring. There are many approach of crossovers like:single-point, two-point, multi-point, cut-splice, uniform, etc., chosen based on application requirement.
- We use cut-splice crossover, which chooses two chromosomes and chooses crossover point which is not identical for both chromosomes. As each parent has different crossover point, offsprings have different chromosome lengths.
- Crossover is used for priority changed context types.
- Crossover operation is followed by mutation(if required). A mutation means altering the value of a gene. Since a gene is a context, during the mutation, we replace the gene with a different context, from the list of available context.
- Mutation is used for new retrieved context.
- Offspring produced by crossover and mutation are candidates for the next generation population.

Flow Diagram of User Context Selection using GA is given in Fig.4.

D. User Certificate Verification

A user may request for the services. UbiSS verifies the UC and facilitates the required user services. User authentication, user access rights and validity are verified. UC are mainly context-bound and later time-bounded.

Reverse UC generation process takes place and FP's are compare with signature for verification, which proves the authenticity of the UC.

IV. Simulation and Results

The proposed authentication scheme using genetic algorithm are simulated on Ubiquitous Museum environment. Ubiquitous Museum environment consists of 100 to 200 nodes, in which:
25-30 nodes are selected as fixed artifacts of the museum,
30-40 nodes as sensors: to retrieve the visitor context information,

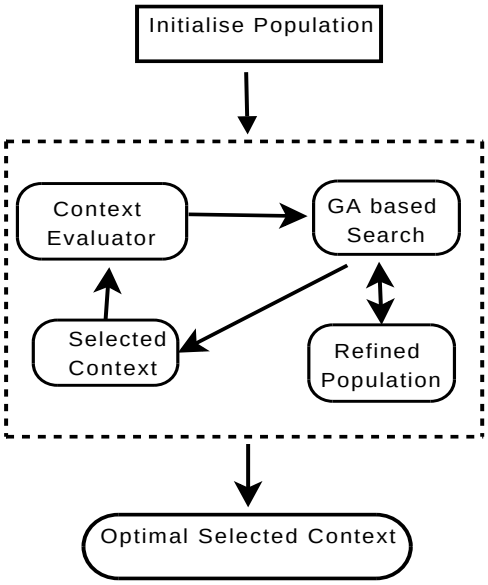

Fig. 4. User Context types Selection using GA

10-20 nodes as stand-by security and service nodes,
Rest nodes are the visitor nodes.

The parameters of GA: Initialization population size is 50; Crossover rate is 0.85; Mutation rate is 0.03. The simulation is written in Java language, and the results are as follows. For context, we have used only user interest, preference, hobbies and physical location. Physical location context is given low priority, as it keeps changing. High priority for the rest.

Fig. 5 shows the selection of context for the user certification using a random method of selection and selection using genetic algorithm. GA based selection seems to give better results.

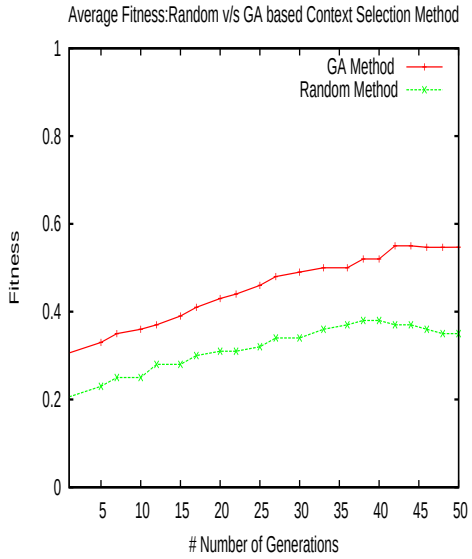

Fig. 5. Average Fitness of context

Fig. 6 shows the number for context used for certification for three users over generation. For each user it uses different number of context elements, which makes the certificate unique. Hence it is a dynamic certification process.

Fig. 7 shows the total certification cost incurred for the its generation. Certification cost depends on number of context

ISBN: 978-988-19252-0-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

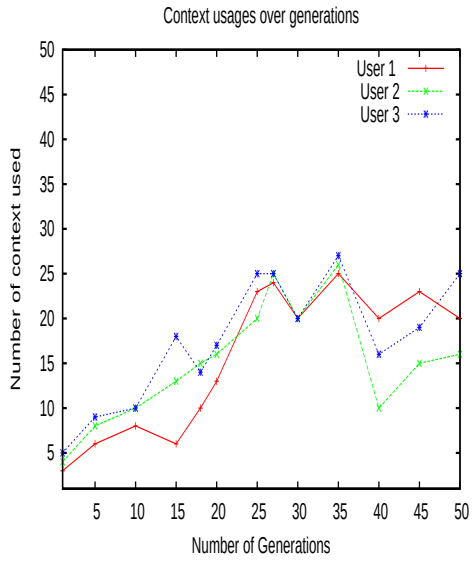

Fig. 6. Context usage

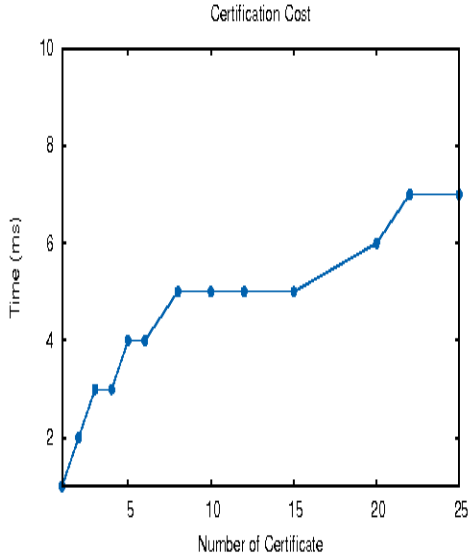

Fig. 7. Certification generation cost

selects and number of generation used for best context selection.

V. Conclusion

UbiSS authentication is based on the user context. The system aim to provide service to the genuine user, hence does not believe in one point authentication. User privileges are directly associated with user current context binded with user identity. As context changes, user certificates adapts to the context and continue to provide services. Genetic algorithm is used find the context to be used for the certification process. As user context changes, new context get added to the gene population and system evolves with the genetic evolution. New evolution gives new set of context and new certificates are generated to meet the user needs.

References

[1] Mari Korkeaaho, *Context Aware Applications Survey*, Department of Computer Science, Helsinki University of Technology, 2000.

[2] A. K. Dey and G. D. Abowd, *Toward a Better Under standing of Context and Context-Awareness*, Proceedings of 1st International Symposium on Handheld Ubiquitous Computing, LNCS, vol.1707, Pages 3047, 1999.

[3] Davies N., Mitchell K., Cheverest K. and Blair G., *Developing a Context Sensitive Tourist Guide*, First Workshop on Human Computer Interaction with Mobile Devices, GIST Technical Report G981, 1998.

[4] Byeong-Ho KANG, *Ubiquitous Computing Environment Threats and Defensive Measures*, International Journal of Multimedia and Ubiquitous Engineering, Vol. 2, No. 1, January, 2007.

[5] S. Dritsas, D. Gritzalis, and C. Lambrinoudakis, *Protecting privacy and anonymity in pervasive computing: trends and perspectives*, Telematics and Informatics, vol. 23, Pages 196-210, 2006.

[6] T. Strang and C. Linnhoff Popien, *A Context Modelling Survey*, 6th International Conference on Ubiquitous Computing, Wksp. Advanced Context Modeling, Reasoning, Management, Sept. 2004.

[7] *OpenID: wikipedia*

[8] Akihiro Takahashi and Yasuo Okabe, *Providing Ubiquitous Networks Securely Using Host Identity Protocol (HIP)*, AINTEC '11, Proceedings of the 7th Asian Internet Engineering Conference, Pages 156-159, ACM, New York, USA, 2011.

[9] Shwetak N. Patel, Jeffrey S. Pierce and Gregory D. Abowd, *A Gesture-based Authentication Scheme for Untrusted Public Terminals* , UIST04, Santa Fe, New Mexico, USA, 2004.

[10] Zhefan Jiang, Kanghee Lee, Sangok Kim, Hyunchul Bae, Sangwook Kim, Soongju Kang, *Design of a Security Management Middleware in Ubiquitous Computing Environments*, Parallel and Distributed Computing, Applications and Technologies(PDACAT), 2005.

[11] A. Varshavsky, A. Scannell, A. E. Lara LaMarca, *Amigo: Proximity-based Authentication of Mobile Devices*, Proceedings of the 9th International conference on Ubiquitous computing, Berlin, Heidelberg, pp. 253-270, (2007).

[12] P. Venkataram and B. Sathish Babu, *An authentication scheme for ubiquitous commerce: A cognitive agents based approach*, In the Proc. of IEEE Network Operations and Management Symposium Workshops, 2008. NOMS Workshops 2008, pp. 248-256, Brazil, Apr. 11, 2008.

[13] J. Wang, J. Yu, D. Li, and Z. Jia, Combining authentication with role-based access control based on IBS, in Computational Intelligence and Security, 2006 International Conference on, vol. 2, nov. 2006, pp. 1475 1480.

[14] P. B. Lim and J. S. Seong, *Method for Authentication of Subscriber using the MAC Address*, Samsung Electronics Co., Ltd., 2004.

[15] K. Gaarder and E. Snekkens, *Applying a formal analysis technique to the ccitt x.509 strong two-way authentication protocol*, Journal of Cryptography, 3(2), Pages 81-98, 1991.

[16] C. Neuman, T. Yu, S. Hartman, K. Raeburn, *The Kerberos Network Authentication System*, RFC4120, July 2005.

[17] O. Raiha, *Genetic Synthesis of Software Architecture*, Ph.D. thesis.

[18] C. E. Shannon, A mathematical theory of communication, The Bell System Technical Journal, vol. 27, pp. 379423, 623656, 1948.

ISBN: 978-988-19252-0-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)