International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: 05 July 2023 Revised: 25 August 2023 Accepted: 15 September 2023

A Novel Context Aware Privacy Provision Algorithm for Hand Held Devices

[1]Thyagaraju G S, [2]H. Manoj T. Gadiyar, [*3]Ashwitha A, [4]Kishor Shivathaya S, [5]M Bharathraj Kumar, [6]Niranjan Mamadapur

[1]Professor and Head, Department of Computer Science & Engineering,
Sri Dharmasthala Manjunatheshwara Institute of Technology, Ujire, 574240, Karnataka, India.
[2]Associate Professor, Department of Computer Science & Engineering,
Sri Dharmasthala Manjunatheshwara Institute of Technology, Ujire, 574240, Karnataka, India.
[*3]Assistant Professor (Senior Scale), Information Technology department,
Manipal Academy of Higher Education (MAHE), Bangalore, India.
*Corresponding Author Email: ashwitha.a@manipal.edu
[4]Assistant Professor, Department of Computer Science & Engineering,
Canara Engineering College, Benjanapadavu, 574219, Bantwal Taluk, Karnataka, India.
[5]Assistant Professor, Department of Electronics and Communication Engineering,
Sri Dharmasthala Manjunatheshwara Institute of Technology, Ujire, 574240, Karnataka, India.
[6]Assistant Professor, Department of Electronics and Communication Engineering,
Sri Dharmasthala Manjunatheshwara Institute of Technology, Ujire, 574240, Karnataka, India.

Abstract-Context-awareness is an emerging area in the current technical world as it adapts mechanisms and interfaces of applications based on consumer preferences as well as the environmental conditions. Various applications of Internet of Things can be perceived in the fields such as but not limited to agriculture, Industry, Medical and Healthcare, Smart Home Appliances, etc. Since last couple of decades use of mobile devices have grown tremendously everywhere in this world. Adding computing capabilities has increased their application to many folds and has made task as well as life simpler than earlier days. These smart-phone embedded with computing features have become an integral part of daily life of people globally. Unprecedented rates of growth were noticed in use of mobile applications on these handheld devices. But adding to the wows, subscribers are usually requested to provide personal and context data, while making use of these mobile utilities. The permission have to be given to access the user location, the contact details as well as the gallery of the mobile storage whenever the new application have to be installed. Due to these conditions applied by the application providers the privacy concern came into being for security experts and organizations. In order to render better services to the users, privacy is an important concern employed. The privacy is enhanced in the context aware applications through the proposed encryption strategies to offer efficient services. In the proposed approach, an active encryption strategies are employed for enhancing the network security.

Keywords*:* Context-awareness; Internet of Things; Privacy**.**

I. INTRODUCTION

In mobile environment, web services of Mobile phones are software application of web services technology or internet [1-2]. These are stated to be web services those implemented on mobile equipment that are circulated over within operators' network, Internet or wireless system. Providing novel personalized amenities to users on the mobile devices is a basic aim of mobile web services like laptop computers, wireless-LAN enabled PDAs [3] and telephones. For promoting an effective networking service, the authentication and privacy are highly significant. The authentication is involved with sharing the keys and sharing the required parameters. In order to provide better security in terms of authentication, advanced techniques are required to be developed to improve the security of context aware applications [4-5]. The process of encryption improves the file security and to access this, right key is required for decryption. These processes render a most significant way to secure the information effectively.

A. Web Services with Context Awareness

The phenomenon of providing contextually coordinated web amenities to cater requested services wants at that moment is referred to as "context-aware web services" [6]. With two perspectives Context can be explained like one from web services and other from service requesters. From latter's perspective, context may be defined as an eco-system influencing requester's service discovery access like requesters' accessible network devices, location, preference and activities.

Their system constitutes various modules like context consumer, context storage, context sensor, context reasoned.

B. Context Awareness Based Mobile Web Services

It is a mobile computing platform where applications could find out and extract benefits of circumstantial data like consumer's time of day, location, user activity with nearby people and devices. Recently many scientists and researchers have observed [7-9], studied and developed various application based on context-aware technology for demonstrating practicality of these novel innovations. There are 2 technologies that enable subscribers to move along with network resources and computing power at hand held wireless communication gadgets and portable computers. By each passing day computing enabled handheld device are shrinking with respect to their sizes in enabling gadgets with mobility couple with impressive computing power, at the same time wireless bandwidth capacity keeps rising.

C. Web Service's Security Limitations

With various advantages granted, web services technology is continuously experiencing critical threats [10-11] like Buffer Overflows, Replay and Capture Attacks, Improper Error Handling, DoS (Denial-of-Service) Attacks, prefix hijacking, Eavesdropping and interruption in Internet because of man-in-the-middle attack.

DDOS attacks include ADDoS attacks and TDDoS attacks where former encompass new generation of DDoS attacks.

The privacy concern security has turn out to be main problem in area of web service technology. There exist various difficulties in web amenities making safety the more complex phenomenon [12-13]. Number of threats could jeopardise confidentiality integrity or availability web services, which can uncover web service's back-end systems that is significantly very important aspect.

Hence, most important study and observation is focussed in web service technology is its security. But at the same time, Web service security requires extra consideration in bigger security problems such as authorization, integrity, confidentiality, authentication, and non-repudiation and validation process.

D. Context Aware Privacy and Security Issues

Context awareness is a process in which the system or system components gather information from its surroundings [14-15]. It collects the data automatically and responds to the dynamically arising situations.

Let us take smart home as a scenario. There are many Internets of things when it comes to smart home which are well built and connected by one or the other smart home builders. Now, all the devices are in IoT will be connected to their server through network. Here, the privacy breach can take place either in the way information is shared with the server or though the network connected hand held devices.

II. LITERATURE REVIEW

A probabilistic infrastructure was proposed by Hayashi et al. [16] with regards to Context-Aware Scalable Authentication (CASA). An active authentication scheme is chosen dynamically by probabilistic framework which caters to a specified security need if provided with passive factors. Depending on passive factors these models can choose active authentication factors which balances usability and security subscribers authentication and validation. Passive multi-factor information could be utilized in modulating asset of lively authentication required in attaining a assumed threshold for security; this became basic concept of CASA.

A suitable structure for the "Purpose Oriented Situation Aware Access-Control (PO-SAAC)" software amenities was provided by Kayes et al. [17]. Here, the model states and mentions about the purpose related conditions and it's relation to situation-specific admission control strategies and protocols. This prototype takes into consideration the states of entities as well as the states of relationships amongst these entities so as to attain context-aware access control.

Various aspects of consumption and schemes to manage context restrictions were provided by Kosala Yapa Bandara et al. [18]. Ontology dependent service provisioning context model was also proposed by him. To ensure availability of contextualization of effectively related characteristics of Web service procedures is a significant goal of this model.

An infrastructure for data privacy and security was presented by Antorweep Chakravorty et al. [19]. It ensures security and privacy from sensor data of smart homes where appliances are connected with internet so as to get remote access and automation of property. Privacy is linked with storage, collection, processing, use, destruction or sharing of personally identifiable information. Saving and keeping personally recognisable information as hashed values which maintains recognisable data from any computing nodes on network with web services.

The study offers three categories: who you are, who you are with, and the objects that are around you are three categories that were offered by Schilit et al. [20]. These context cases are often used when starting to study context systems.Context as environmental features of overall currently existing situation were explained by Hull et al. [21]. Context as user's position and alignment, target of their attention, emotional state, time and date, people and objects in their surroundings were defined by Dey [22].

Context as a group of parameters and environmental conditions that define the behaviour or cause of an application to fail and concern the consumer was introduced by Chen and Kotz [23]. In some of particular systems such definitions are generally very broad and complicated in applying. Ryan et al. [24] and Abowd et al. [25] definitions are identical and depicts relationship with their personal opinions. Context includes not only a subscriber's identity information and location, but even her/his time information and environments this explanation was put up by Ryan et al. [24].

But, Abowd et al. [25] proceeded in arguing that term environment must be substituted by activity. A basic question of what is happening in specific conditions can be answered by activity they thought, contrary to environment which cannot provide it. This research is in line with Abowd et al. [25]'s description; hence, context personifies users' conditions by responding when, what, who and where correspondingly. Based on today's hand-held device's technological advances, gathering information related to context is no longer a difficult or complicated problem.

A privacy preserving block chain enabled in 5G networks was proposed by Wan et al. [26]. In this technique, machine learning (ML) was employed to preserve the data proficiently. A federated learning based privacy preserving ML was projected to prevent the raw data transfer. In accordance to this, Wasserstein generative adversial network (WGAN) with differential privacy was developed to prevent unsolicited malicious attack by understanding the context. The controllable random noise fulfilling with differential privacy requirements was proposed. Better trade-off between privacy protection and data utility had obtained.

The privacy-preserving and sparsity aware location was introduced by Meng et al. [27] for collaborative recommender systems. In this presented technique, location founded collaborative recommendation procedure was presented to attain better trade-off between privacy. A random perturbation method was projected to prevent the data user's quality of service. Additionally, region aggregation method was established to prevent the specific user location. Furthermore, location aware method was introduced to generate service and location relationship to progress location aware predictions.

Consequently, mobile context-awareness emphasizes on developing and creating applications that can be benefitted from contextual data. A context-aware application should consist of significant and large ability in observing surrounding environment.

The Sensors are components that are equipped on mobile devices, like Wi-Fi, real-time, Bluetooth and GPS. Opacity tools known as Actuators are tools deployed for privacy protection application. They mainly focuses on protecting identity of consumer, and to reduce influence of disclosed personal information by, as an instance, obstructive critical attacks and encrypting personal information. Rules are enforced on a particular environment.

Conversely, in a mobile environment, the overall factor differs significantly more. The consumer's behaviour may vary and may utilize diverse amenities or actions at diverse places and times zones. Additionally, smart phones store valuable personal information such as passwords and photos as well as important personal information (ie, current location information).This leads to raise in mobile subscribers concerns on their data safety and privacy.

III. A SURVEY OVER CONTEXT-AWARE-PRIVACY

A realization of Smart Environment IoT solicitations and strategies will always include risks associated to consumer privacy. These issues are addressed in many related works earlier as shown in Table 1.

However, the derived solution from these works may not deliberate consumer characteristics including privacy preferences, location dynamicity etc.

To address these contexts aware privacy issues the importance should be on the user centric method while framing privacy policies as well as application installation.

So, Context aware privacy service is a prominent way to apply consumer centric secrecy preferences.

Here, we have developed a novel algorithm to address some dynamically raised context-aware privacy issues.

TABLE 1: COMPARISON OF PREVIOUS WORK CARRIED OUT ON CONTEXT AWARE PRIVACY AND SECURITY AS A SERVICE IN IOT ENVIRONMENT

Reference	**Privacy**	**Authentication**	**Authorization**	**As a service**
[1]	Yes	No	Yes	No
[2]	No	Yes	Introduced	No
[3]	Yes	No	No	No
[4]	Introduced	Introduced	Introduced	No
[5]	Yes	Introduced	Introduced	No
[6]	Introduced	No	Yes	No
Proposed	Yes	Yes	Yes	Yes

Some of the previous works are compared with the proposed work in terms of diverse context aware sectors. From the table, it is clear that the proposed model performs better in all sectors including privacy, authentication, services and authorization whereas the existing models fails to perform well in some sectors. Figure 1 shows privacy control architecture.

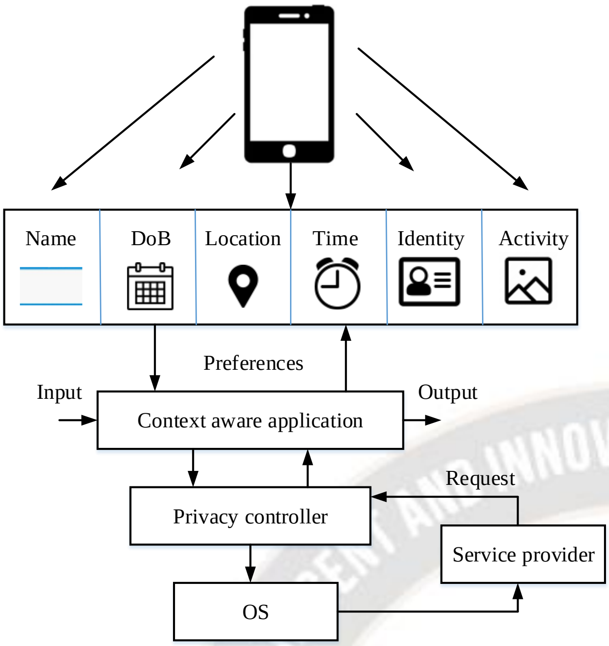

Figure 1. Privacy Control Architecture

IV. NOVEL ALGORITHM APPROACH

In mobile recommendation systems, we place a high value on privacy. Our two interfaces are both traditional and privacy-friendly in their design. The interfaces adapt in response to the situation. The algorithm determines on the necessity of context aware privacy provision to the consumers based on his interest. The data of proposed privacy preservation approach are prevented using Advanced Encryption Standard (AES) and Message Digest 5 (MD5) to provide an end-to-end security over hand held devices. These encryption methodologies can prevent the users from several network attacks like middle attack, phishing attacks and so on. The AES are composed of block ciphers which tends to encrypt and decrypt the data correspondingly. The secret key ciphers utilize the similar key for both encryption and decryption and so both sender as well as receiver knows the secret key. All the key lengths are made sufficient to preserve the information. The AES encryption is highly reliable whereas MD5 renders better assurance of transferred files. The MD5 algorithm is a significantly used cryptographic hash function that can process a variable length message over a fixed output length. The proposed algorithm is highly novel when compared to the previous approaches whereas better context aware privacy, authentication and authorization can be obtained through the proposed model. Better network services can be rendered to the users on comparison with existing methods. Through the proposed model, dynamic decision-making can be allowed during the operation of a mobile device. Diverse strategies such as local network capabilities, user preferences and the mobile terminal capabilities can be effectively improved. Better security can be rendered as the public users cannot access the application in any ways because of strong security deployment.

/* This method assesses whether a privacy-friendly interface is necessary in the context. */

Step 1: Login towards the application by utilizing username and password.

Step 2: Encrypt the login credentials using AES and MD5 techniques

Step 3: Location based context identification

Step 4: If the identified context is of interest and within the range of 100 meters

Step 5: The Hand Held Device (HHD) is switched to silent mode and phone calls get blocked automatically

Step 6: After the context is out of desired range a call back message is notified to the sender, without interference of the recipient

Step 7: Then the HHD is switched to normal mode

Step 8: If the user (consumer) is unable to login to the context aware application, he/she will not able to access the privacy controller

Step 9: Decrypt the data if correct credentials are given as the input.

The consumer should register to the context aware application with all the required credentials before being able to login to the application.

A. Outer Framework

Figure 2 shows the outer framework of interface.

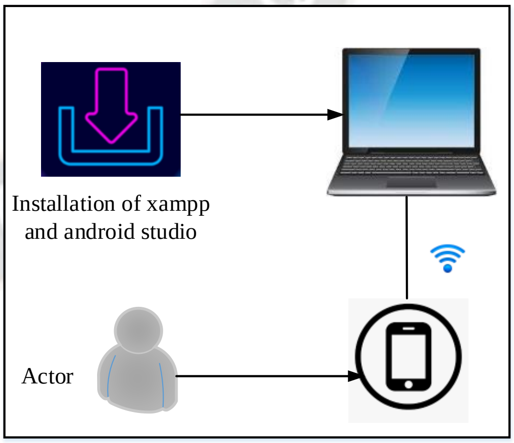

Figure 2. Interface

B. Overview

The components that are required to run this context aware privacy application are wi-fi / internet service, laptop and mobile devices. Initially we install both android studio and Xampp to the system, and same wifi should connect to both laptop and mobile phones. After that turn off all the firewalls in the system, now run the context privacy app in the mobile phones, here user has to login with username and password along with the location (location is enable). Based on the location range of 100m the required privacy is provided to the user. Example: If user is in temple then based on the location the phone calls get blocked and phones are automatically switched to silent mode. Both the user of the device and the caller will be alerted on the call for possible call back after the user is out of 100 meters range from the interest area.

V. RESULTS & ANALYSIS

Context-aware applications are a type of mobile application that adapts its behavior to the user's current situation, such as where they are, who they are with, what time of day it is, and so on.

The paper depicts an application that is conscious of the user's context when it comes to privacy. If a user creates an account with that app, it will ask for username, phone number, password, email address, and other information. After logging in to that app, it will automatically block calls and put the phone in silent mode depending upon the location of user. In the prototype built the context privacy program runs on smart phones, but the device must be connected to a laptop before logging in. After connecting the device to the system, turn off the system's firewalls (Domain network, Private network, Public network), then enable the developers' option in the smart phone. Finally, while running the project in Android Studio, the same Wi-Fi must be linked to both the system and the device.

VI. PSEUDO IMPLEMENTATION

Algorithm: Context aware privacy

```
Begin
Input: Login credential data
Output: Secured data access
    Initialization of context aware application
    Logging into the application
       Enter username and password
Encryption using AES and MD5 approaches
              \\ Encrypted data
Location based context identification
       IF identified context < 100 meters then
       Switch the handheld devices to silent mode
              \\ Block the call automatically
         IF identified context > Range
              \\ Message notification to sender
         Then Switch the handheld devices to normal mode
       End If
        End If
            If the credentials are correct then
                \\ Login to the application
Else
                \\ cannot be accessed
        End if
end
```

VII. CONCLUSION

The paper shows a novel context-aware privacy algorithm for mobile users that can help protect their personal data by utilizing the respective contextual preferences. Contextual information of 100 real-time mobile users were gathered as part of this research work over a one-year period. Research contributes to understanding that context, context-aware measures that combine information about time and place, can be visualized as a unique identifier. In previous works, contextual privacy has raised concerns about consumer privacy. As users are constantly being tracked by location-based applications, this generates a large amount of potentially sensitive information about consumers of handsets. The context aware algorithm is introduced in the hand held devices to manage privacy issues in user context. Here, the privacy controller module makes the decision on behalf of the user, set a decision and will notify the underlying operating system. The service provider is then communicated by the operating system. Here, our major focus is on the context data that is either specified by the user or obtained from the sensors. The proposed algorithm has manifested its potential to address threats to certain extent. The algorithm has shown an increase user level authentication and ease of use. Therefore it may help major business practitioners. The algorithm when implemented at real time provides protection with respect to privacy. It also has authentication security and ease of use as its performance criteria which make it dissimilar to its most previous instantiations. This work is presented to meet the privacy necessities that has to be satisfied in context aware application. Some of the existing privacy preserving research works has been reviewed and analyzed the challenges security. In this work, the complexities are overcome with encryption strategies over context aware applications for privacy preservation in prevalent environments.

REFERENCES

[1] V. Alagar, A. Alsaig, O. Ormandjiva and K. Wan, Context-Based Security and Privacy for Healthcare IoT, In: 2018 IEEE International Conference on SmartInternet of Things. IEEE, Xi'an, China, pp. 122-128, 2018.

[2] Y. Ashibani, D. Kauling and Q. H. Mahmoud, A context-aware authentication service for smart homes, In: 2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC). IEEE, Las Vegas, NV, USA, pp. 588-589, 2017.

[3] M. Barhamgi, C. Perera, C. Ghedira and D. Benslimane, User-centric Privacy Engineering for the Internet of Things, IEEE Cloud Computing, vol. 5, no. 5,pp.47-57,2018Available: 10.1109/mcc.2018.053711666.

[4] E. de Matos, R. T. Tiburski, L. A. Amaral, F. Hessel, Providing Context-Aware Security for IoT Environments Through Context Sharing Feature, In: 2018 17th IEEE International Conference on Trust, Security and Privacy in

Computing and Communications/ 12th IEEE International Conference on Big Data Science and Engineering. IEEE, New York, NY, USA pp. 1711-1715, 2018.

[5] R. Neisse, G. Steri, G. Baldini, E. Tragos, I. N. Fovino, M. Botterman, Dynamic Context-Aware Scalable and Trust-based IoT Security, Privacy Framework, In: Internet of Things - From Research and Innovation to Market Deployment, River Publishers Series in Communication, River Publishers, pp.199-224, 2015.

[6] J. L. H. Ramos, J. B. Bernabe, A. F. Skarmeta, Managing context information for adaptive security in iot environments, In: 2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops, IEEE pp. 676-681, 2015.

[7] R. Mizouni, M. Matar, Z. Mahmoud, S. Alzahmi and A. Salah, A framework for context-aware self-adaptive mobile applications SPL, Expert Systems with Applications, vol. 41, no. 16, pp. 7549-7564, 2014. Available: 10.1016/j.eswa.2014.05.049.

[8] J. Krumm, A survey of computational location privacy", Personal and Ubiquitous Computing, vol. 13, no. 6, pp. 391-399, 2008. Available: 10.1007/s00779-008-0212-5.

[9] J. Sterngold, Say Goodbye to All Those Passwords-Businessweek, BusinessWeek: Online Magazine. 2011.

[10] C. Cortes and V. Vapnik, Support-vector networks, Machine learning, vol. 20, no. 3, pp. 273–297, 1995.

[11] V. Vapnik, The nature of statistical learning theory, Springer Science & Business Media. 2013.

[12] P. Lingras and C. J. Butz, Precision and recall in rough support vector machines, IEEE International Conference on Granular Computing, IEEE, pp. 654–654, 2007.

[13] L. Pevzner and M. Hearst, A Critique and Improvement of an Evaluation Metric for Text Segmentation, Computational Linguistics, vol. 28, no. 1, pp. 19-36, 2002 Available: 10.1162/089120102317341756.

[14] A. Osterwalder and Y. Pigneur, Business model generation: a handbook for visionaries, game changers, and challengers, John Wiley & Sons, New York, USA. 2010.

[15] T. Sylla, M. A. Chalouf, F. Krief and K. Samaké, Towards a context-aware security and privacy as a service in the internet of things, InIFIP International Conference on Information Security Theory and Practice, Springer, Cham pp. 240-252, 2019.

[16] E. Hayashi, S. Das, S. Amini, J. Hong and I. Oakley, Casa: context-aware scalable authentication, In Proceedings of the Ninth Symposium on Usable Privacy and Security, pp. 1-10, 2013.

[17] A. Kayes, J. Han and A. Colman, OntCAAC: An Ontology-Based Approach to Context-Aware Access Control for Software Services, The Computer Journal, vol. 58, no. 11, pp.3000-3034, 2015 Available: 10.1093/comjnl/bxv034.

[18] K. Y. Bandara, M. Wang and C. Pahl. An extended ontology-based context model and manipulation calculus for dynamic web service processes. Service Oriented Computing and Applications. vol. 9, no. 2, pp. 87-106, 2015.

[19] A. Chakravorty, T. Wlodarczyk and C, Rong, Privacy preserving data analytics for smart homes, In2013 IEEE Security and Privacy Workshops, pp. 23-27, 2013.

[20] B. Schilit, N. Adams, and R. Want, Context-aware computing applications, In First workshop of Mobile Computing Systems and Applications, IEEE, pp. 85–90 (1994).

[21] R. Hull, P. Neaves, and J. Bedford-Roberts, Towards situated computing, *First* International Symposium on Wearable Computers, IEEE, pp. 146–153, 1997.

[22] Dey, A.K. Context-aware computing: The CyberDesk project. Proceedings of the AAAI 1998 Spring Symposium on Intelligent Environments, pp. 51–54, 1998.

[23] G. Chen, D. Kotz and others. A survey of context-aware mobile computing research, Technical Report. TR2000-381, Dept. of Computer Science, Dartmouth College, Hanover, NH, USA. 2000.

[24] N. Ryan, J. Pascoe and D. Morse, Enhanced reality fieldwork: the context aware archaeological assistant, Bar International Series, vol. 750, pp. 269–274, 1999.

[25] G. D. Abowd, A. K. Dey, P. J. Brown, N. Davies, M. Smith and P. Steggles, Towards a better understanding of context and context-awareness, Handheld and ubiquitous computing, Springer, pp. 304–307, 1999.

[26] Y. Wan, Y. Qu, L. Gao and Y. Xiang, Privacy-preserving blockchain-enabled federated learning for b5g-driven edge computing. Computer Networks, vol. 204, pp. 108671, 2022.

[27] Meng, S., Qi, L., Li, Q., Lin, W., Xu, X., and Wan, S. Privacy-preserving and sparsity-aware location-based prediction method for collaborative recommender systems. Future Generation Computer Systems, vol. 96, pp. 324-335, 2019.