An adaptive approach for preserving privacy in context aware applications for smartphones in cloud computing platform

H. Manoj T. Gadiyar (✉ hmanojtgadiyarphd@gmail.com)  
Sri Dharmasthala Manjunatheshwara Institute of Technology

Thyagaraju G.S  
Sri Dharmasthala manjunatheshwara Institute of Technology

R H Goudar  
Visvesvaraya Technological University

Research Article

Keywords: Context-Aware, Privacy, active defence, Privacy Protection and Mobile phones

Posted Date: January 10th, 2023

DOI: https://doi.org/10.21203/rs.3.rs-1600119/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License. Read Full License
An adaptive approach for preserving privacy in context aware applications for smartphones in cloud computing platform

*1a,bH. Manoj T. Gadiyar, 2Thyagaraju G. S. & 3R H Goudar

*1aAssistant Professor,
Department of Computer Science & Engineering,
Sri Dharmasthala Manjunatheshwara Institute of Technology,
Ujire – 574240, Karnataka, India
bVisvesvaraya Technological University,
Belagavi, Karnataka, India
2Sri Dharmasthala Manjunatheshwara Institute of Technology,
Ujire – 574240, Karnataka, India
3Visvesvaraya Technological University,
Belagavi, Karnataka, India
*Email: hmanojtgadiyarphd@gmail.com

Abstract: With the widespread use of mobile phones and smartphone applications, protecting one’s privacy has become a major concern. Because active defensive strategies and temporal connections between situations relevant to users are not taken into account, present privacy preservation systems for cell phones are often ineffective. This work defines secrecy maintenance issues similar to optimizing tasks, thereby verifying their accuracy and optimization capabilities through a hypothetical study. Many optimal issues arise while preserving one’s privacy and these optimal issues are to be addressed as linear programming issues. By addressing linear programming issues, an effective context-aware privacy-preserving algorithm (CAPP) was created that uses an active defence strategy to determine how to release a user’s current context to enhance the quality of service (QoS) regarding context-aware applications while maintaining secrecy. CAPP outperforms other standard methodologies in lengthy simulations of actual data. Additionally, the minimax learning algorithm (MLA) optimizes the policy users and improves the satisfaction threshold of the context-aware applications. Moreover, a cloud-based approach is introduced in our work to protect the user’s privacy from third parties. The obtained performance measures are compared with existing approaches in terms of privacy policy breaches, context sensitivity, satisfaction threshold, adversary power, and convergence speed for online and offline attacks.

Keywords: Context-Aware, Privacy, active defence, Privacy Protection and Mobile phones.

1. Introduction
Mobile phones are used extensively, and apps are commonly produced for smartphones. “Context-aware applications specifically help users by providing contextually relevant tailored services (Hussain T and Alawadhi R (2020)), (Shu J (2018)). Context-aware applications may use sensors (e.g., GPS) to determine their owner’s location and state. These sensory data may be used to determine a user’s context or condition. For example, a user’s position may be relayed via GPS, their movement assessed by accelerometers, and their voice and scene captured by cameras and microphones. Context-aware applications may use the inferred context to provide context-aware tailored services (Bai G, et al. (2010)). Health Monitor can track daily activity and intelligently mutes the phone without the help of the user. Context-aware applications improve people’s lives and convenience yet also compromise privacy. Some untrusted aware applications may be highly prone to leakage of user’s context privacy to the adversary. These adversaries may sell the user privacy for
commercial purposes, resulting in a reduction of QoS of the context applications. In reality, most users would not reject enable context-aware applications to access linked sensory data owing to the convenience they give. Thus, avoiding the danger of context-privacy exposure while delivering context-related services is becoming more important (Pingley A, et al (2012)).

Constantly changing human situations and actions in everyday life make it difficult to maintain context-privacy for mobile phones (Zhang H, et al (2015)). As a matter of fact, a Markov chain may represent temporal relationships across human settings. By introducing temporal correlation among present contexts, can estimate the past and future usage of context applications more efficiently. Because the naïve method ignores temporal connections between user contexts, it fails to secure critical user contexts. With MaskIt (Qingsheng Z, et al (2007)), sensitive and non-sensitive contexts may be silenced to reduce temporal connections between them. MaskIt’s ability to hide additional contexts reduces the QoS given by context aware smartphone applications. This approach uses passive defence, which inevitably reveals some information to opponents. Determining whether the hidden circumstances are sensitive or not is irrelevant to an opponent. Recent proposals include aggressive defence programmes. To reduce temporal correlations across contexts, the deception approach is introduced in each context called FakeMask. FakeMask releases scenarios that are not genuine but have significance (i.e. the user has a likelihood of being in that context at that moment) (Stephen R (2014)). An increased number of actual contexts leads to greater service quality for consumers with such a deception strategy. As a result, it is not suitable for mobile devices (Pandit A, et al (2014)).

In recent years, many researchers have been fascinated with cloud computing (Phan TN, et al (2018)) due to the efficient outcome for protecting privacy from the third party. Only a few types of research are undertaken for optimal policy users, but increasing the satisfaction threshold remains a challenging approach. To prevent the attack from adversary, an efficient approach is required for a better outcome. Although a few types of research are taking place in this field, there also arises high leakage of user privacy. These major drawbacks motivate us to develop an efficient approach to preserve the user’s privacy from adversary attacks. A lightweight privacy preservation approach is introduced to develop temporal correlation among every user context to protect one’s privacy more effectively. We formulate the context-privacy issue for mobile phones as an optimization problem and then prove its validity. It is followed by a near-optimum problem (linear programming) to speed up the execution time. By addressing the linear programming issue, we build an efficient context-aware privacy preserving algorithm (CAPP) that can select how to release a user’s current context to optimize the QoS of context-aware applications with privacy preservation. To analyze the method performance, we run extensive simulations, and the simulation results show the suggested algorithm is effective and efficient. Our proposed work undergoes the following major contributions to show the better QoS of the developed model:

- This research work mainly focuses on developing a novel approach for preventing leakage of data in context-aware applications for smart phones using cloud computing.
- An effective context-aware privacy-preserving (CAPP) algorithm is introduced to address the linear programming issue.
- Minimax learning algorithm (MLA) is emphasized to optimize the policy users and improve the satisfaction threshold.
- To preserve the user’s privacy, the cloud computing approach is evaluated. It mainly creates a firewall between the adversary and the user.
- The evaluation of the proposed work based on privacy policy breaches, context sensitivity, satisfaction threshold, adversary power, and convergence speed for both
online and offline attacks are investigated and compared with traditional approaches.

2. Literature Review

Some of the recently published papers are surveyed below:

Wang et al. (Wang R and Tao D (2019)) studied the context-aware implicit authentication of smartphone users based on multi-sensor behaviour. In this method, multi-sensor data like accelerometer, gyroscope, magnetometer, time stamp, pressure and touch size were initially encapsulated to determine one’s behaviour. Here, gesture and touch features were drawn from sensed data using a statistical and distance calibration approach. The features are fused using the weighted sum fusion rule, and a one-class support vector machine (SVM) was used to classify the outcome. For experimentation, 1000 sensed data from 80 participants were considered. The overall equal error rate (EER) attained was about 0.0071% in the experimental scenario. However, this method was highly suffered due to leakage of the privacy to the third party.

Alawadhi et al. (Alawadhi R and Hussain T (2019)) performed the method toward privacy protection in context aware environment. In this method, the decision making process was introduced to monitor privacy behaviour and personal data usage. This method undergoes three stages: service classifier, privacy preference manager, and privacy controller. The privacy preference module places the privacy preference and analyses the user’s data usage. The next module uses service providers under trusted, untrusted and under investigation. The privacy controller detects the usage of data based on service providers. The overall false positive rate (FPR) attained was about 1.5% in the experimental scenario. However, this method suffered due to high optimization problems.

Hayashi et al. (Hayashi E (2013)) performed the context aware scalable authentication (CASA). This method introduced a probabilistic framework to satisfy the security based on passive factors. The Bayesian framework was introduced here to verify the authentication in both passive and active approaches. For experimentation, a mobile phone of 1000 users was taken and analyzed. The overall satisfaction threshold attained was about 68% in the experimental scenario. However, this method suffered due to high attacks from the adversary.

Kayes et al. (Kayes ASM (2014)) defined the purpose oriented situation aware access control framework for software services (PO-SAAC). In this method, purpose oriented situation method (POSM) was introduced to state the entity and distinguish between the entity and the user’s intention. SAACPM was evaluated to support the control according to the related situations. Also, ontology based framework implementation was developed for identifying information related to the access control. In the experimental scenario, the memory size utilized about 1600 KB based on the response time. However, this method suffered due to high computational complexity with increased memory size.

Sylla et al. (Sylla T (2021)) investigated secure and trustworthy context management for context aware security and privacy in the IoT (SETUCOM). In this method, device trust management (DTM) was introduced based on context aware and privacy as a service (CASPaaS). The context information was secured using a Bayesian network and fuzzy logic, and it was considered the lightweight hybrid system. The elliptic curve integrated encryption scheme (ECIES) algorithm generated the security. Advanced encryption standard (AES) was evaluated for context information encryption. In the experimental scenario, the overall time taken to protect the information is about 1200ms. However, this method suffered due to insecurity of the user’s privacy and its highly occurs optimization problems. Table (1) illustrates the comparison of various existing approaches.
| Author & reference | Method | Performance | Merits | Demerits |
|--------------------|--------|-------------|--------|----------|
| Wang et al.        | The context-aware implicit authentication of smartphone users based on multi-sensor behaviour. | EER attained was about 0.0071%. | Low error rate and consumes only low power. | Leakage of the privacy to the third party. |
| Alawadhi et al.    | The method towards the privacy protection in context aware environment. | FPR attained was about 1.5%. | Low FPR and high efficiency. | High optimization problem. |
| Hayashi et al.     | The context aware scalable authentication (CASA). | The satisfaction threshold attained was about 68%. | Easy framework for smooth analysis. | High attack from the adversary. |
| Kayes et al.       | The purpose oriented situation aware access control framework for software services (PO-SAAC). | The memory size utilized about 1600 KB based on the response time. | Memory size is reduced for a low database. | High computational complexity with increased memory size. |
| Sylla et al.       | The secure and trustworthy context management for context aware security and privacy in the IoT (SETUCOM). | The overall time taken to protect the information takes about 1200ms | Low time requirement compared to other approaches. | Insecurity of the privacy of the user and it highly occurs optimization problems. |

**Problem formulation**

The literature above highly affects the previous approaches due to major drawbacks such as high leakage, privacy loss, and slow process. In (Wang R and Tao D (2019)), the author studied the context-aware implicit authentication of smart phone users based on multi-sensor behaviour to the privacy of the user’s context. However, this method was highly prone to leakage of users’ privacy and lack of firewall. In (Alawadhi R and Hussain T (2019)), the author performed the method toward the privacy protection in context aware environment to preserve the environmental context of the user. However, this method suffered due to optimal issues that resulted in leakage of user privacy to the adversary. In (Hayashi E (2013)), the author proposed the context aware scalable authentication (CASA) to enhance the context application by providing a firewall. However, this method was highly suffered due to user’s
location privacy leakage. In (Kayes ASM (2014)), the purpose oriented situation aware access control framework for software services (PO-SAAC) was introduced to control one’s privacy attacks from a third party. However, this method suffered due to programming complexity to preserve one’s context privacy. In (Sylla T (2021)), the author proposed secure and trustworthy context management for context aware security and privacy in the IoT (SETUCOM) to improve the QoS of the context applications. However, this method suffered due to the high complexity process and the lack of preserving location privacy more effectively.

Few researchers were undertaken to protect users’ privacy based on cloud computing. The aforementioned related paper is efficient and shows a better outcome in terms of privacy preservation, but there also arises some leakage due to less improvement in the applied strategy. An effective novel approach needs to be introduced to preserve privacy to overcome this issue. Our proposed method gives a clear solution for data protection with better accuracy.

3. Proposed Method

Context aware is the computation of the current situation and information about the environment, places, things that anticipate urgent needs, situate awareness, usable contents and experiences. In this work, we developed a novel approach to prevent an attack from an adversary concerning users privacy. Initially, we introduced CAPP to enhance the quality of service (QoS) regarding context-aware applications. Then, the MLA algorithm is emphasized to equalize the optimal policy and improve the satisfaction threshold of the proposed work. Our proposed work introduces cloud computing to encrypt users’ privacy from a third party. Figure (1) illustrates the framework of the proposed model.

![Figure 1: Framework of the proposed method](image-url)
Cloud computing is the collection of network servers coordinated with the aid of the internet. The cloud uses firewalls as privacy protection around assets to prevent intruding of third parties. To carry out this evaluation, real smartphones with traces of 94 users to find out the convergence speed of the algorithm. Our paper mainly focuses on online and offline attacks due to continuous changing times and user variability.

3.1 Privacy problems in context aware privacy preservation

The private contexts are said to be the context subsets in which leakage is considered the major drawback for the smartphone user. In order to prevent the leakage of privacy, the user must control the emitted information using middleware privacy preservation. Many existing approaches are introduced to overcome the leakage of the user’s privacy. Privacy-preserving middleware is used to access the context-aware middleware for the users, but this middleware does not require any permission to access the user’s data. Usually, the released data with granularity leaks the privacy of the user. Hence the accuracy of the context recognition is also reduced. The context-aware apps are mainly used for commercial purposes and are considered the adversary. The adversary is a third party intrusion, mainly focusing on reducing the user’s utility by adding multiple attacks. The attacks mainly undergo two stages offline and online attacks.

The third party gets the user’s personal information such as behavioral contexts, GPS location information, etc. These third parties sell the information for commercial purposes, and users are unaware that the attack leads to a privacy breach. In online attacks, the third party collects the sensed data from the user and understands the user’s behavior based on the collected data. According to the behavior, the third party forces the user or makes the user indulge in blackmail or leads to violence.

3.1.1 State transition for online attacks

For the online attack, the adversary’s strategy is unknown to the user, and the user blindly believes the adversary’s strategy from the existing attacks. There are many reasons for the dependence on previous attacks. The third party collects the last context based on the previous approach. Then the present information is coordinated with the past information based on the proposed algorithm. Hence the user should encapsulate the adversary’s attacks and which information has been attacked. The attacked time is denoted by \( n \), which clearly shows the time the data gets leaked. The attack of the previous information is indicated as \( W_{R^n} \), the value of \( W_{R^n} \) is 1 or 0. If the adversary successfully collects the information is denoted as \( D_{n-1} \). The state transitions for the online attacks at the time \( n \) is given by,

\[
R^n = \{W_{R^n}, D_{n-1}\}.
\]

3.1.2 State transition for offline attacks

In an offline attack, the adversary gets the user’s personal data such as personal behavior contexts, environmental context, GPS location etc. The adversaries sell one’s personal information for money and lead to a privacy breach, and it is unknown to the user. The time \( n \) of the user’s action is given by, \( a^n_h = \{a^n_{h,1}, \ldots, a^n_{h,E}\} \), the granularity of the sensor’s data is denoted as \( a^n_{h,E} \in [0,1], \forall E=1, \ldots, E \). Here, E denotes the complete sensors for the purpose of recognition. The recognition of the context in terms of accuracy with the limit ranges from \( t (0 \leq t \leq 1) \) is given by,

\[
t = \sum_{E=1}^{E} E_t a^n_{h,E}.
\]
Here, $\{E_c: \forall E\}$ denotes the weight of the context sensitivity based on context recognition accuracy.

The adversary’s attacking capability needs to choose the correct subset of regretting the sensed data. A formula gives the time $n$ with the adversary actions as,

$$a^n_{b} = \{a^n_{a,1}, a^n_{a,E}\}$$  \hspace{1cm} (2)

Here, $a^n_{b,e}$ denotes the $E$th sensor of the retrieved data. The adversary actions with limited power adversary given mathematically as,

$$\sum_E a^n_{b,j} \leq L, 0 \leq a^n_{a,j} \leq 1, \forall E$$  \hspace{1cm} (3)

Here, $L$ denotes the adversary power limitations. Based on the limit $L \leq E$, the third party can capture the sensed data. Hence this adversary is said to be an unlimited power adversary.

The behavior of the adversary in online attacking the user can be determined in a probabilistic manner, and it is given by,

$$Pb[R^n | a^n_{h,a}] = Pb[Wr^{a+1} | Wr^n, a^n_{h,a}] Pb[D^{a+1} | D^n] = Pb[WR^{a+1} | a^n_{h,a}] Pb[D^{a+1} | D^n]$$  \hspace{1cm} (4)

The offline attack in case of adversary based on the probabilistic manner is given by,

$$Pb[R^{a+1} | a^n_{h,a}] = Pb[D^{a+1} | D^n]$$  \hspace{1cm} (5)

3.2 Proposed context aware privacy preservation algorithm

The optimization problem gets converted into a linear programming problem to improve the convergence speed. To overcome the linear programming problem, the CAPP algorithm is introduced. It generates the active policy users and increases the service quality for context aware applications with user privacy.

![Figure 2: Architecture of privacy aware](image_url)

Figure (2) shows the architecture for privacy aware. The service provider gives a request to the PC about the priority. The PC does not request permission from the user directly and sends the requests through the PC module. The module provides the decision and notifies it to
the OS that communicates with the SP consecutively. The user’s privacy is stored in the privacy preference manager (PPM). It enables the user to set the privacy and sensitivity to context aware apps.

- ✓ Dividable
- ✓ Not dividable
- ✓ To be Established
- ✓ Cannot be established.

Dividable means the user feels comfortable for giving one’s personal information. Not dividable denotes that the user feels insecure in sharing one’s information. The data to be established depicts that when the user uses the application source for the first time, he sets the location permission to be dividable or cannot be dividable to the application. It cannot be established indicates that the user is unable to express to set the context priority that is sharable or not.

The SC module describes the category of the service provider based on the context request and how it is divided among the SP. SP undergoes 3 stages: hopeful, hopeless, and examining. The hopeful SP is the one who asks only necessary information from the user. The hopeless SP is the one who asks for unnecessary that are not required for the adversary. The adversary is tested for hopeful or hopeless SP in the investigation category.

The PC module senses the user when the hopeless SP attacks the personal data.

The deciding operation is done by three operation

- Allow – allow access to context request
- Deny – prevent access from context requests.
- Approximation- allow access to approximate the value based on the context request.

| ALGORITHM FOR CONTEXT AWARE PRIVACY PRESERVATION |
|--------------------------------------------------|
| Step 1: Initialize service provider (SC)         |
| Step 2: Allow request for PC to preference       |
| Step 3: if, users data is sharable               |
|   Allow PC to get service provider from SC      |
| Step 4: else, users data not sharable            |
|   Send decision to OS                           |
|   End                                           |
| Step 5: if, SP is trusted                        |
|   Allow permission to access users data         |
|   Send decision to OS                           |
|   End                                           |
| Step 6: else, SP is not trusted                  |
|   Access deny                                   |
|   Send decision to OS                           |
|   End                                           |
| Step 7: do, investigation and approximate range of SP |
|   Send decision to OS                           |
|   End                                           |
| Step 8: else,                                    |
|   Allow request for PC to preference             |
| Step 9: if, SP is trusted                        |
|   Suggest to user to access the data             |
|   Gets users decision from PC                   |
|   Send decision to OS                           |
|   End                                           |
The algorithm selects how to reveal a user’s context while protecting their privacy. Even if an opponent knew the Markov model with associated probability matrices of emissions, they couldn’t determine the original context from CAPP’s output context sequence. Because privacy ensures a condition with which an adversary can never know the user when within the sensitive environment.

3.3 Mini max learning algorithm
The minimax algorithm is a step by step process that aids the computer in working intelligently instead of not learning automatically. It mainly helps to improve the satisfaction threshold for the proposed approach.

The pair of the optimal policy is given by, \( \phi^* = \{ \phi_h^*, \phi_a^* \} \) for the game based context privacy is achieved by overcoming the convergence problem.

\[
\tilde{U}^{n+1}(W_r) = (1 - \beta^{n+1})\tilde{U}^n(W_r) + \beta^{n+1}G[s_h(r,a_h^n,a_a^n) + \lambda \tilde{U}^n(W_r')] \tag{6}
\]

Based on the eqn (1), using the learning approach, the \( \tilde{U}^{n+1}_h(W_r) \) is obtained, and this can be obtained using upgraded rule based on the Q-learning approach.

\[
\phi^* = \arg \max_{\phi_h} \min_{\phi_a} \{ s_h(r,a_h) + \lambda \sum_{W_r} (Tr(W_r'/a) \tilde{U}^{\delta'}(W_r')) \} \tag{7}
\]

The algorithm of minimax learning is shown below:

---

**Mini-max learning algorithm**

**Input:** the stochastic game for context aware privacy given by, \( \Psi \)

**Output:**

// (i) Start
1. \( n \leftarrow 0, W_r^n = 0 \); 
2. \( \tilde{U}^n(W_r=0) \leftarrow 1, \tilde{U}^n(W_r=1) \leftarrow 1 \); 
3. Start the pair for policy \( \phi^*_a \) distributed based on uniform \( a_h^n, a_a^n \); 
   // (ii) Recursion 
4. Iterate 
5. Choose the action pair \( \{a_h^n, a_a^n\} \) according to \( \phi^* \);
6. Upgrade \( W_r^{n+1} \) after each user’s taken into consideration as \( \{a_h^n, a_a^n\} \)
7. Upgrade \( \tilde{U}^{n+1}(W_r) \) convergence state notation as, based on equation (2).
8. Upgrade the optimized policy as $\phi^{n+1}$ based on the equation (1) with upgraded stated notations;
9. $n \leftarrow n + 1$;
10. Until equalize

The learning rate is indicated as, $\beta^n \in [0,1]$ for the convergence of learning algorithm, must degrade the high time operation. Set $\beta^n = \frac{1}{n} \tilde{U}^{n+1}(WR)$ that is used as an approximate value and updated continuously until it equalizes.

Algorithm 1 evaluates the learning algorithm in an equivalent state, denoted as, $\tilde{U}_h^{\phi^*}(WR)$. Initially, set the equalization state values as 1 and make the uniform distribution among the players of each policy. After that, the equivalent state values are continuously repeated based on equations (1) and (2). This repetition helps to occur optimal policy among the policy pair.

4. Results and discussion

Our context-aware privacy-preserving algorithm (dubbed CAPP) was developed and compared with currently present algorithms of privacies such as EfficientFake (Pandit A, et al (2014)) and MaskSensitive, MaskIt (using the hybrid check) (Stephen R(2014)). Basic method’s MaskSensitive, which hides or suppresses all sensitive circumstances during the release of a non-sensitive one. The entire simulation was done using MATLAB 8.1 platform, executing on Windows 8.1 and has a 1.80 GHz processor of an Intel Core with a memory of 8 GB. Dataset employed in the simulation in this research is based on actual traces of humans: a dataset of Reality Mining [37], containing fine-grained movement information for hundred employees and students at MIT during 2004-2005 academic duration. Some of the user’s GPS location context is taken from the reality mining dataset to analyze the performance of the proposed method. Consideration of 91 users was undertaken by us, having a minimum of one-month data plan for a complete 11091 day of time span. The trace length for the average, low and high numbers of users, are 122, 30 and 269 days, respectively. The number of locations per user based on high, low, and average is 40, 7 and 19.

4.1 Analysis of performance metrics for the proposed model

To analyze the performance of the proposed method, a Markov chain is given to each user to train and assess the protect the privacy context for every user. Because of the inadequacy of previous beliefs and the probability of emission, privacy may not be ensured while gathering the user’s trace. We can ensure that the user’s privacy is preserved once. We use the privacy value, which is set at 0.1, as a simulation parameter. It was to be noted as a higher privacy parameter, and then lower will be user privacies guarding levels with additional actual sensitive information being revealed. Selecting sensitive environments may be done in one of two ways. Unless otherwise mentioned, we pick sensitive circumstances pertaining to every user selected randomly, referred to as sensitive, unless otherwise noted. Alternatively, for each user, we select a place with the greatest probability of prior as the user’s house, marking that sensitive, dubbed home as sensitive. Because the expected amount in released real context was utility about privacy-preserving technique, we utilized normalized utility as evaluation, defined as the proportion of release actual context. It’s worth noting that context-aware applications give better service when their utility is greater. Identically, we split the amount of sensitivity contextual within the user’s context sequence, which got discontinued by the user’s context sequence length in evaluating privacy breaches. Three Methods, Mask It (Qingsheng Z, et al (2007)), CAPP (Vahdat-Nejad H (2019)) and Efficient Fake (Chakraborty
S, et al. (2014)), and everyone guarantees no violation of privacy, according to the definition. Mask because of the lack of assumption for the presence of temporary connections across the user’s context, Sensitive is unlikely to be able to ensure the desired privacy.

![Figure 3: comparison for privacy policy breaches (home as sensitive).](image1)

(a) MaskSensitive  (b) MaskIt  (c) NaiveFake  (d) CAPP (e) Proposed

![Figure 4: Comparison for privacy policy breaches (sensitive as random).](image2)

(a) MaskSensitive  (b) MaskIt  (c) NaiveFake  (d) CAPP (e) Proposed

In the first example, we compare CAPP’s and MLA privacy violations to those of alternative techniques. With certain conditions, three contexts were chosen by us randomly as sensitive about every user, whereas, in the other, we selected each user’s house as sensitive. It’s worth noting that a user’s house has the greatest previous belief, indicating that the user must spend most of their time inside the house rather than elsewhere. In the preceding two instances, Figures (2) and (3) shows released and repressed contexts in average proportions.
by different methods. All sensitive circumstances were surpassed by Mask Sensitive in entire instances, as can be seen in the images. Even though not every sensitive context was revealed within Mask Sensitive, opponents that understand the contexts of the Markov chain can predict around 40–60% sensitive contexts out of suppressed ones in both cases. The major reason is that the temporal connection across contexts gives an adversary enough information to conclude a greater post belief that can surpass correspondingly preexisting belief by privacy parameter. On the other hand, CAPP, EfficientFake, and MaskIt ensure that privacy is maintained. Some sensitive and non-sensitive contexts are repressed and released in CAPP, EfficientFake, and MaskIt. CAPP also releases a higher percentage of genuine situations than MaskSensitive, MaskIt, or EfficientFake. MaskIt compromises less than 20% of Mask Sensitive’s functionality to ensure anonymity, as seen in the numbers.

However, compared to Mask Sensitive, both EfficientFake and CAPP boost usefulness by about 20% while ensuring anonymity. The fundamental reason for this is that the new deception strategy makes it harder to antagonist in deriving posterior beliefs, allowing more genuine contexts to be released. Despite the fact that CAPP and EfficientFake were both formalized in linear programming problems, Ours CAPP outperforms EfficientFake techniques with both instances in terms of average utility. There are two primary reasons for this. The first difference is that in EfficientFake, the aim is to optimize emission probability solely. Still, with CAPP, the aim was to maximize the value of utility for a provided period of time. Secondly, Efficient Fake’s space of resolution has shrunk significantly. The emission probability matrix’ Shape in EfficientFake was reduced to a vectored representation, thereby significantly reducing the solution’s precision in EfficientFake, resulting in lower utility than CAPP. On the other hand, CAPP does not shrink the solution space, allowing us to find a superior optimized solution.

![Graph](image)

**Figure 5:** Tradeoff for Privacy-utility (home as sensitive).
The usefulness of our CAPP is then compared to that of other techniques with various privacy settings ranging from 0.05 to 0.3. We pick separate sensitive settings in the trials, just as we did in the previous ones: the sensitive environment for one person is their home, while the other is chosen at random. With the reduction in the privacy requirement, we anticipate utility to rise. Figures 4 and 5 show that utility grows slowly as the number of people rises in both circumstances.

Moreover, we may show that, for similar privacy values, every solution executes in the best way within 2nd case. The context of random was designated sensitive, compared with the first situation, when the home was designated as sensitive. Because locations of every having greatest belief of prior were picked sensitive context in the first scenario in Figure (4), the number of sensitive contexts was greater than the 2nd situation in Fig (5), in which sensitive context was selected at random. CAPP and Efficient Fake should release more fake contexts in the first case to give identical privacy levels. However, when related to other methods, our CAPP outperforms them all due to its close approximation of the problem’s optimum solution.
Figure (7) represents the comparison of sensitive context and the sum of the discounted payoff for an online attack. When the sensitive context percentage increases, the myopic strategy (Wang X (2020)) gets highly decreased. The users of high sensitive contexts result in more privacy leakage. But this strategy shows high leakage in the case of the privacy policy. In the fixed strategy (Wang W and Zhang Q (2016)), the same percentage of sensitive context results in the same sum of the discounted payoff. However, this strategy shows poor outcomes because of its insecure privacy. It is due to the constant quality of service, and it controls the payoff discount in case of a fixed strategy. In the case of the MDP approach (Gu B (2019)), it is the same as the myopic strategy.

However, this approach works more efficiently in the case of privacy preservation than the myopic strategy. But, this method shows a lie outcome based on context aware privacy preservation. Our proposed model shows better results in protecting the privacy of the user. By increasing the percentage of the sensitive context to 1, the sum of the payoff discount gets very much increased to 2.9 because of using an optimal algorithm with cloud computation.

![Figure 8: Comparison of satisfaction threshold and payoff discount](image)

Figure (8) compares the satisfaction threshold and sum of the discounted payoff. The satisfaction threshold is compared with the existing application based on the sum of discounted payoff. From the graph, we can see that if sum of the discounted payoff gets lower, the satisfaction threshold gets very much lower. If the satisfaction threshold gets increased, the quality of service gets lower. The existing approach results in low-quality service by comparing the proposed model with the myopic strategy. If the service quality decreases, it is harder to better accuracy in the outcome. Hence the satisfaction threshold must be lower to prevent the loss of leakage in privacy. In the case of the MDP approach, there attains a better quality of service. However, this method shows some drawbacks in hiding the information from the third party. Our proposed model shows better privacy protection as the satisfaction threshold is only 0.15.
Figure 9: Different context sensitivity based on optimal policies

Figure (9) represents the different context sensitivity based on optimal police based on online policy. Here, a, b illustrated in the graph denotes the released and leaked data. With the smaller context sensitivity of 0.25, the optimal policy achieves 1. When the context sensitivity becomes higher by about 0.87, the optimal policy attains a negligible value. In the case of smaller context sensitivity, the service quality variance improves, and vice versa, the loss of privacy dominates. Suppose both a and b go down, the context sensitivity increases. Due to this, the user chooses a more optimized strategy to protect their privacy efficiently. From the graph, it is clear that if the satisfaction threshold increases, the context sensitivity decreases. Suppose the user receives only low-quality service if the threshold becomes lower. Understanding the satisfaction threshold is considered an important parameter while developing context-aware privacy protection approaches.

Figure 10: Different adversaries with optimal policies

Figure (10) illustrates the different adversaries with optimal policies for the offline attack. Here, L denotes the adversary power of the privacy policy. Considering, at L=1, attains poor adversary power due to high leakage of privacy of the user. In myopic strategy, the discounted payoff with different adversary power is higher than our proposed work. For efficient usage of context aware applications, the sum of discounted payoff should be too
low. From the graph, we can understand that the sum of discounted payoff gets degraded, resulting in no leakage. In existing approaches, compared with the limited adversary power, the performance of the adversary power with unlimited power gets very worse. Mainly, the adversary with unlimited power occurs more leakage, and hence the user selects another strategy to protect their privacy.

**Figure 11:** Comparison of sensitive context and payoff discounts

Figure (11) illustrates the comparison of sensitive context and payoff discounts. As per the graph, when the sensitive context percent increases, the discounted payoff’s sum gets degraded. This denotes that sensitive users have to use the more encrypted forms to preserve user privacy. When the sensitive context percent increases in myopic strategy, the discounted payoff’s sum gets degraded slowly. But this approach does not show better accuracy in preserving the user’s privacy under offline attacks. In fixed strategy, the sum of discounted payoff gets diminished gradually with an increase in sensitive contexts. But this approach uses high complexity in protecting one’s privacy from the third party. The MDP approach is also the same as the other existing approach because of the lack of new approaches to protect the privacy of the user. Our proposal shows a better outcome because it performs effectively in preserving the privacy of the user.

**Figure 12:** Comparison of satisfaction threshold and payoff discounts
Figure (12) compares the satisfaction threshold and sum of the discounted payoffs. As per the graph, when the satisfaction threshold (accuracy) increases, the sum of the discounted payoff gets decreases slowly in the case of myopic strategy. This shows that this strategy is not suitable for preserving the privacy of the user due to low service quality. In the case of fixed strategy, the sum of discounted payoff decreases significantly with increased accuracy. This approach shows a lack of service quality due to the absence of a slow encryption process. Considering the MPD approach, the sum of the discounted payoff gets decreased with an increase in accuracy but is not efficient due to a lack of preserving privacy from the third party. When the sum of the discounted payoff gets decreased, the accuracy is very high. This shows that our proposed method with cloud computing helps the user protect their privacy effectively.
Figure 13: Comparison of payoff discount and for varying iteration. (a) Sum of discounted payoff at L=1. (b) Sum of discounted payoff at L=2. (b) Sum of discounted payoff for unlimited power.

Figure (13a), (13b), (13c) shows the sum of discounted payoff at L=1, L=2 and with unlimited power. As per the graph, the discounted payoff gets reduced when the adversary’s power gets increased. It is due to the increase of L, and the adversary can access more data. Hence it is influenced by the adversary to attack the user successfully. Considering the releasing data with less granularity shows the lower service quality or the user should depend on the same approach to protect user’s privacy. This leads to more loss in privacy of the user and less payoff. The existing approaches like myopic, fixed and MDP approach more leakage in the privacy of user due to low satisfaction threshold. Our proposed method shows good encryption in protecting the user’s privacy because of high satisfaction threshold.

Figure 14: Convergence speed based on CDF.

Figure (14) illustrates the cumulative distribution function (CDF) of various iterations in order to learn the optimal policy of the reality mining dataset. The operating speed of the proposed work is analyzed for 220 iterations. For the MPD process, the convergence speed is
analyzed with $10^5$ iterations. This shows that our proposed algorithm has a higher convergence speed than the MDP process. The proposal algorithm’s equivalent state value helps reduce the high dimensionality for learning the process efficiently.

4.2 Discussion
This research mainly focuses on developing a novel approach for preventing data leakage in context aware applications for smartphones using cloud computing. An effective context aware privacy preserving (CAPP) algorithm is introduced to address the linear programming issue. Minimax learning algorithm (MLA) is emphasized to optimize the policy user’s and improve the satisfaction threshold. To preserve the privacy of the user, the cloud computing approach is evaluated. It mainly creates a firewall between the adversary and the user. The performance of the proposed work is compared with existing approaches like Naivefake, MaskIt, EfficientFake and CAPP models. But this method suffered due to multiple drawbacks. To protect the privacy of the user is not an easy task. Many issues like the third party intrude and cracking may occur due to the lack of advancements in sensor networks.

In the context-aware implicit authentication of smartphone users based on the multi-sensor behaviour. But this method was suffered due to leakage of the privacy to the third party. EER attained was about 0.0071%. In the method toward the privacy protection in context aware environment. However, this method suffered due to high optimization problems in context aware scalable authentication (CASA). However, this method suffered due to high attacks from the adversary. FPR) attained was about 1.5%. An aware access control framework for software services (PO-SAAC) was introduced in the purpose-oriented situation. However, this method suffered due to high computational complexity and increased memory size. The memory size utilized about 1600 KB based on the response time in the secure and trustworthy context management for context aware security and privacy in the IoT (SETUCOM). However, this method suffered due to insecurity of the user’s privacy and it’s highly occurs optimization problems. The overall time taken to protect the information is about 1200ms. The evaluation of the proposed work based on privacy policy breaches, context sensitivity, satisfaction threshold, adversary power, and convergence speed for both online and offline attacks are investigated and compared with traditional approaches. Because of its outstanding performance avoids leakage and privacy loss in smartphones because of its outstanding performance.

5. Conclusion
The challenge of context-aware privacy preservation for cellphones is addressed in this study. We verify the validity and optimality of our formulation through theoretical analysis by formalizing the context privacy preservation issue as an optimization problem. We present an effective, close-optimized strategy where a linear programming problem was created to further speed up the computation. A context-aware privacy preserving algorithm (CAPP) was presented due to the linear programming issue being solved. We show that our suggested CAPP provides much more value than existing techniques while respecting the user’s $\delta$-privacy policy via thorough experimental evaluations on actual mobility traces. A cloud-based approach is introduced in our work to protect the privacy of the user from a third party. In addition to this, a minimax learning algorithm is emphasized for improving the accuracy of the context aware application and improving the optimal policy of the users. The performance measures obtained are compared with existing approaches in terms of privacy policy breaches, context-sensitivity, satisfaction threshold, adversary power, and convergence speed for online and offline attacks. One exciting future project would be to develop an online context released judgment system that can generate faster and most effective judgments.
depending just on the user’s current context while maintaining anonymity. Because this research focuses on preserving privacy for a single user, a future project will provide a privacy preservation technique that considers user interactions, given that people have group mobility.

**Compliance with Ethical Standards**

**Funding:** No funding is provided for the preparation of manuscript.

**Conflict of Interest:** Authors *H. Manoj T. Gadiyar & Thyagaraju G. S, R.H. Goudar,* declares that they have no conflict of interest.

**Ethical Approval:** This article does not contain any studies with human participants or animals performed by any of the authors.

**Consent to participate:** All the authors involved have agreed to participate in this submitted article.

**Consent to Publish:** All the authors involved in this manuscript give full consent for publication of this submitted article.

**Authors Contributions:** All authors have equal contributions in this work

**Availability of data and materials:** No data Availability

**References**

Alawadhi R and Hussain T (2019) A Method Toward Privacy Protection in Context-Aware Environment. Procedia Computer Science 151: 659-666.

Bai G, et al. (2010) Context-aware usage control for android. International Conference on Security and Privacy in Communication Systems. Springer, Berlin, Heidelberg.

Chakraborty S, et al. (2014) {ipShield}: A Framework For Enforcing {Context-Aware} Privacy. 11th USENIX symposium on networked systems design and implementation (NSDI 14).

Gu B, Gao L, Wang X, Qu Y, Jin J and Yu S (2019) Privacy on the edge: Customizable privacy-preserving context sharing in hierarchical edge computing. IEEE Transactions on Network Science and Engineering 7 (4): 2298-2309.

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

Hussain T and Alawadhi R (2020) A Privacy Protection System in Context-aware Environment The Privacy Controller Module. Proceedings of the 22nd International Conference on Information Integration and Web-Based Applications & Services.

Kayes ASM, Han J and Colman A (2014) PO-SAAC: A purpose-oriented situation-aware access control framework for software services. In International Conference on Advanced Information Systems Engineering, Springer, Cham 58-74.

Pandit A, et al (2014) CAPPA: Context Aware Privacy Protecting Advertising-An Extension to CLOPRO Framework. 2014 IEEE International Conference on Services Computing. IEEE.

Phan TN, et al (2018) A context-aware privacy-preserving solution for location-based services. 2018 International Conference on Advanced Computing and Applications (ACOMP). IEEE.

Pingley A, et al (2012) A context-aware scheme for privacy-preserving location-based services. Computer Networks 56 (11): 2551-2568.

Qingsheng Z, et al (2007) Research on context-aware architecture for personal information privacy protection. 2007 IEEE International Conference on Systems, Man and Cybernetics. IEEE.

Shu J, Zheng R and Hui P (2018) Cardea: Context-aware visual privacy protection for photo
taking and sharing. Proceedings of the 9th ACM Multimedia Systems Conference.

Stephen R, Charles PJ and Kumar SBR (2014) A review on privacy control techniques in context-aware web services. International Journal of Advanced Research in Computer Science & Technology (IJARCAST’2014) 2 (3): 222-225.

Sylla T, Chalouf MA, Krief F and Samaké K (2021) SETUCOM: Secure and Trustworthy Context Management for Context-Aware Security and Privacy in the Internet of Things. Security and Communication Networks 2021.

Teixeira L, et al (2014) A rule-based methodology and assessment for context-aware privacy. 2014 IEEE 6th International Conference on Awareness Science and Technology (iCAST). IEEE.

Vahdat-Nejad H, Izadpanah S and Ostadi-Eilaki S (2019) Context-aware cloud-based systems: design aspects. Cluster Computing 22 (5): 11601-11617.

Wang R and Tao D (2019) Context-aware implicit authentication of smartphone users based on multi-sensor behavior. IEEE Access 7: 119654-119667.

Wang W and Zhang Q (2016) Privacy preservation for context sensing on smartphone.” IEEE/ACM Transactions on Networking 24 (6): 3235-3247.

Wang X, Garg S, Lin H, Kaddoum G, Hu J and Hossain MS (2020)PPCS: An Intelligent Privacy-Preserving Mobile-Edge Crowdsensing Strategy for Industrial IoT. IEEE Internet of Things Journal 8 (13): 10288-10298.

Zhang H, et al (2015) CLPP: context-aware location privacy protection for location-based social network. 2015 IEEE International Conference on Communications (ICC). IEEE.